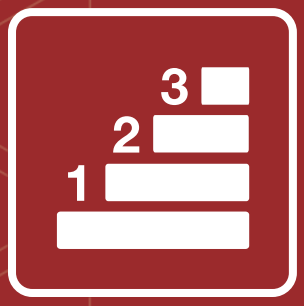


FORTINET
High Performance Network Security

FortiOS™ Handbook - Getting Started

VERSION 5.6.0

FORTINET DOCUMENT LIBRARY

http://docs.fortinet.com

FORTINET VIDEO GUIDE

http://video.fortinet.com

FORTINET BLOG

https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT

https://support.fortinet.com

http://cookbook.fortinet.com/how-to-work-with-fortinet-support/

FORTIGATE COOKBOOK

http://cookbook.fortinet.com

FORTINET TRAINING SERVICES

http://www.fortinet.com/training

FORTIGUARD CENTER

http://www.fortiguard.com

FORTICAST

http://forticast.fortinet.com

END USER LICENSE AGREEMENT

http://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK

Email: techdocs@fortinet.com

Thursday, April 20, 2017

FortiOS™ Handbook - Getting Started

01-560-142188-20170330

TABLE OF CONTENTS

Change Log

Date	Change Description
March 30, 2017	Initial FortiOS 5.6 release.

Introduction

This guide explains how to get started with a FortiGate, and examines basic configuration tasks and best practices in these sections:.

- Installation discusses installing a FortiGate in your network.
- Using the GUI highlights features of the graphical user interface (GUI).
- Using the CLI provides an overview of the command line interface (CLI) for FortiOS. If you are new to the FortiOS CLI, this section provides a high level overview of how to use this method of administration.
- FortiGate Inspection Mode summarizes proxy-based and flow-based inspection modes.
- Fortigate LED Specifications presents a short guide to LED status indicators.
- introduces you to FortiGate models 30-90, also known as the Entry Level models.
- Basic Administration explains basic tasks for setting up a new FortiGate and for updating firmware.
- Next Steps lists resources available to help you with more advanced FortiGate configurations.

Differences between Models

Before you get started, note that not all FortiGate models have the same features. This is especially true of the desktop or entry-level models: FortiGate / FortiWiFi models 30 to 90. If you are using one of these FortiGate models, you may have some difficulties accessing certain features. Preliminary information on entry-level models is available below. Consult your model's Quick Start Guide or hardware manual for further details.

Additionally, users should know that FortiGate models differ principally by the names used and the features available.

Entry-level models

The entry-level, or desktop, models can connect to the internet in two simple steps. They also have a number of features that are only available using the CLI, rather than appearing in the GUI.

- Quick installation using DHCP
- CLI-only features

Names

Naming conventions may vary between FortiGate models. For example, on some models the hardware switch interface used for the local area network is called **lan**, while on other units it is called **internal**.

Features

Certain features are not available on all models. Additionally, a particular feature may be available only through the CLI on some models, while that same feature may be viewed in the GUI on other models.

If you believe your FortiGate model supports a feature that does not appear in the GUI, go to **System > Feature Select** and confirm that the feature is enabled. For more information, see Feature Select on page 45.

For more information about features that vary by model, please see the Feature / Platform Matrix.

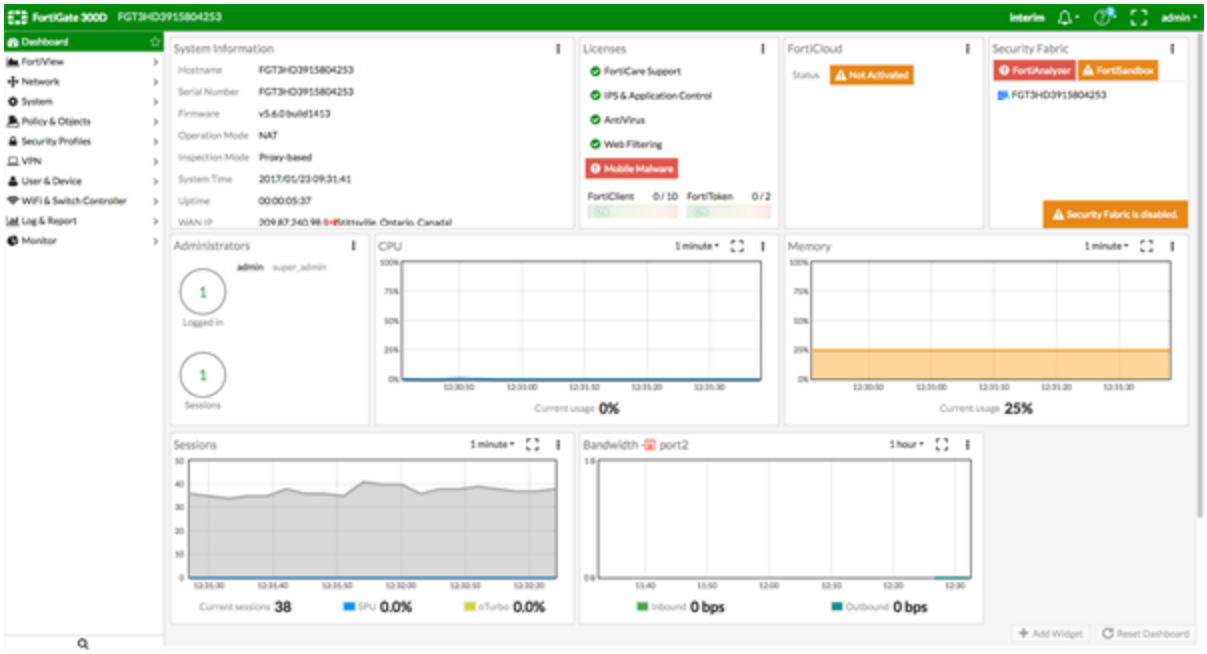
What's New in FortiOS 5.6

This chapter describes new features added to FortiOS 5.6.

The FortiOS 5.6 **Dashboard** has a new layout with a Network Operations Center (NOC) view with a focus on alerts. Widgets are interactive; by clicking or hovering over most widgets, the user can get additional information or follow links to other pages.

Enhancements to the GUI dashboard and its widgets are:

- Multiple dashboard support.
- VDOM and global dashboards.
- Updated resize control for widgets.
- Notifications moved to the top header bar (moved existing dashboard notifications to the header and added additional ones).
- Reorganization of **Add Widget** dialog.
- New **Host Scan Summary** widget.
- New **Vulnerabilities Summary** widget that displays endpoint vulnerability information much like the FortiClient Enterprise Management Server (EMS) summary.
- Multiple bug fixes.



Features that were only visible through old dashboard widgets have been placed elsewhere in the GUI:

- Restore configuration.
- Configuration revisions.

- Firmware management.
- Enabling / disabling VDOMs.
- Changing inspection mode.
- Changing operation mode.
- Shutdown / restart device.
- Changing hostname.
- Changing system time.

The following **widgets are displayed by default**:

- System Information
- Licenses
- FortiCloud
- Security Fabric
- Administrators
- CPU
- Memory
- Sessions
- Bandwidth

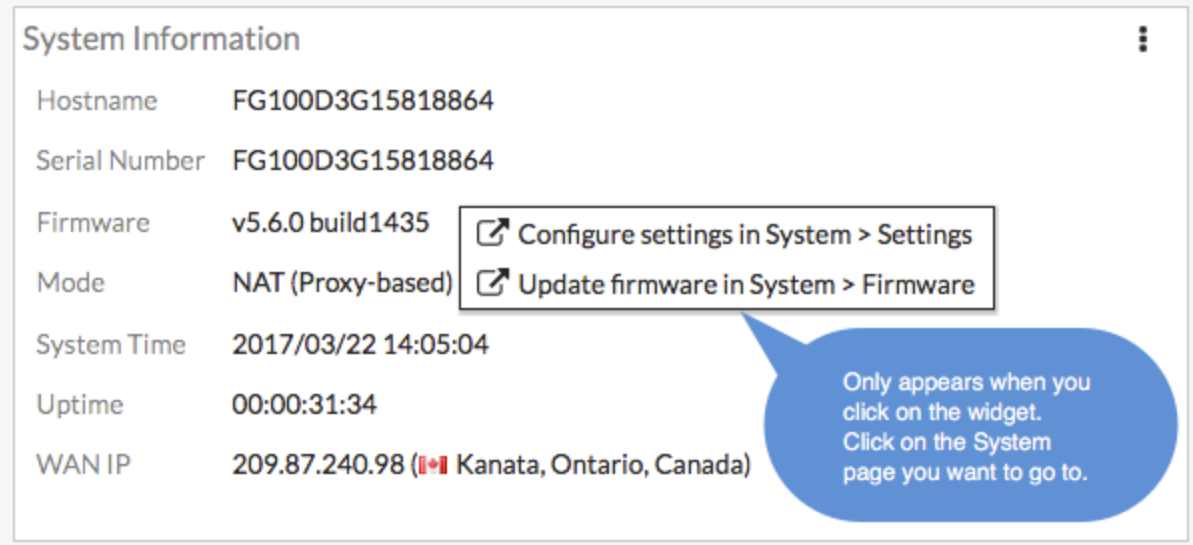
The following **optional** widgets are available:

- Interface Bandwidth
- Disk Usage
- Security Fabric Risk
- Advanced Threat Protection Statistics
- Log Rate
- Session Rate
- Sensor Information
- HA Status
- Host Scan Summary
- Vulnerabilities Summary

The following widgets have been **removed**:

- CLI Console
- Unit Operation
- Alert Message Console

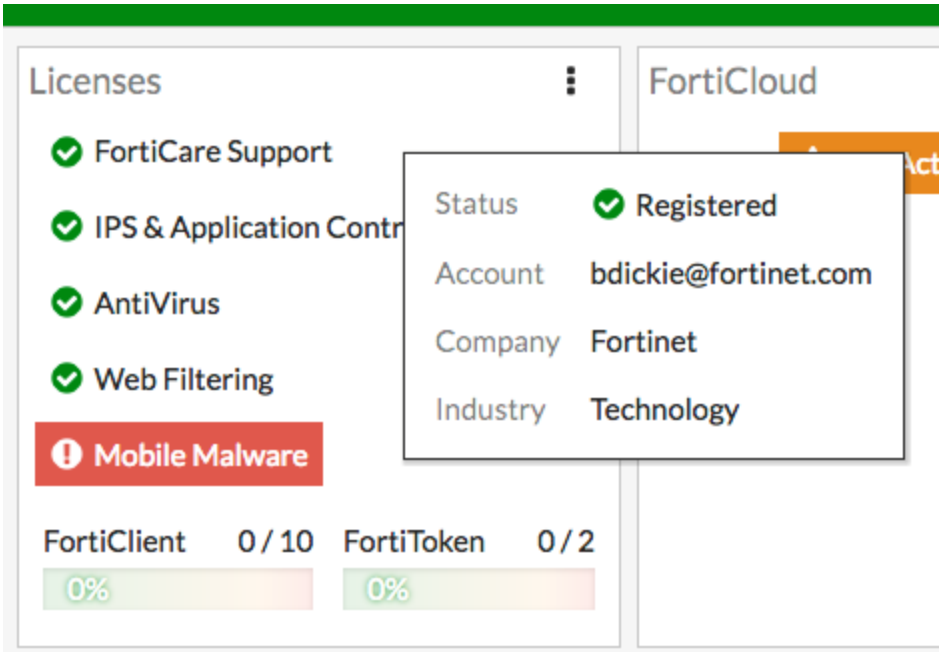
System Information



Licenses

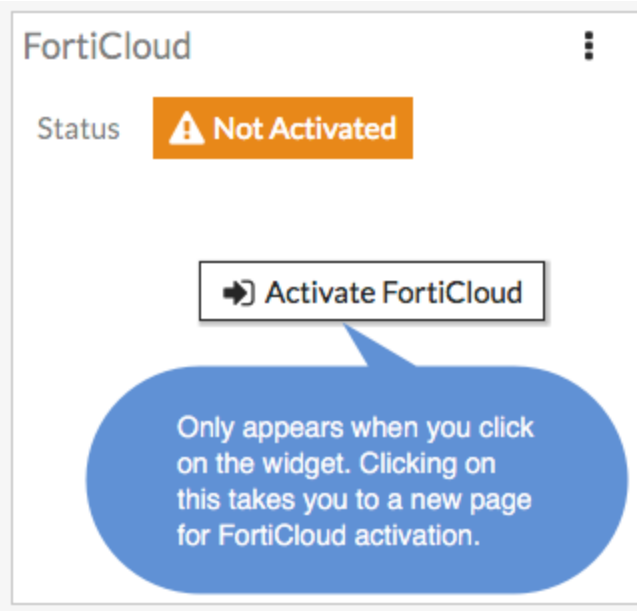
Hovering over the **Licenses** widget will cause status information (and, where applicable, database information) on the licenses to be displayed for **FortiCare Support**, **IPS & Application Control**, **AntiVirus**, **Web Filtering**, **Mobile Malware**, and **FortiClient**. The image below shows **FortiCare Support** information along with the registrant's company name and industry.

Clicking in the **Licenses** widget will provide you with links to other pages, such as **System > FortiGuard** or contract renewal pages.



FortiCloud

This widget displays FortiCloud status and provides a link to activate FortiCloud.

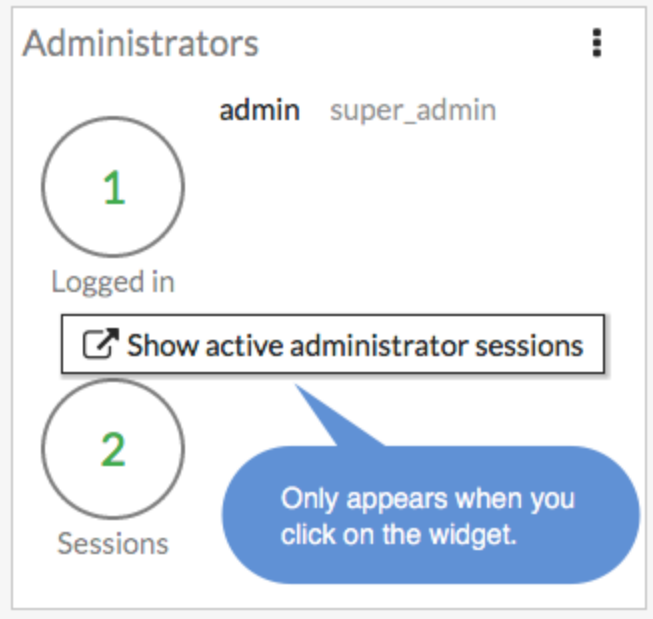


Security Fabric

The **Security Fabric** widget is documented in the Security Fabric section of the **What's New** document.

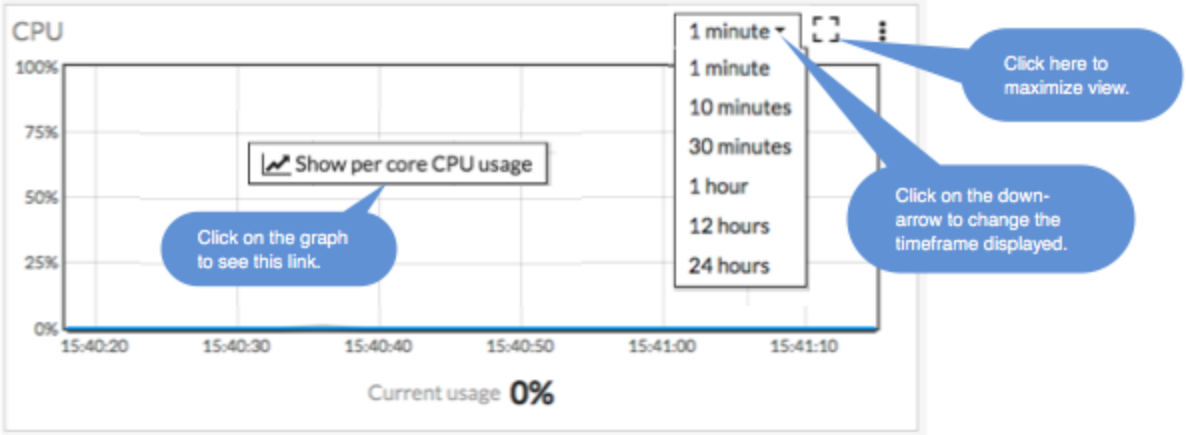
Administrators

This widget allows you to view which administrators are logged in and how many sessions are active. The link directs you to a page displaying active administrator sessions.



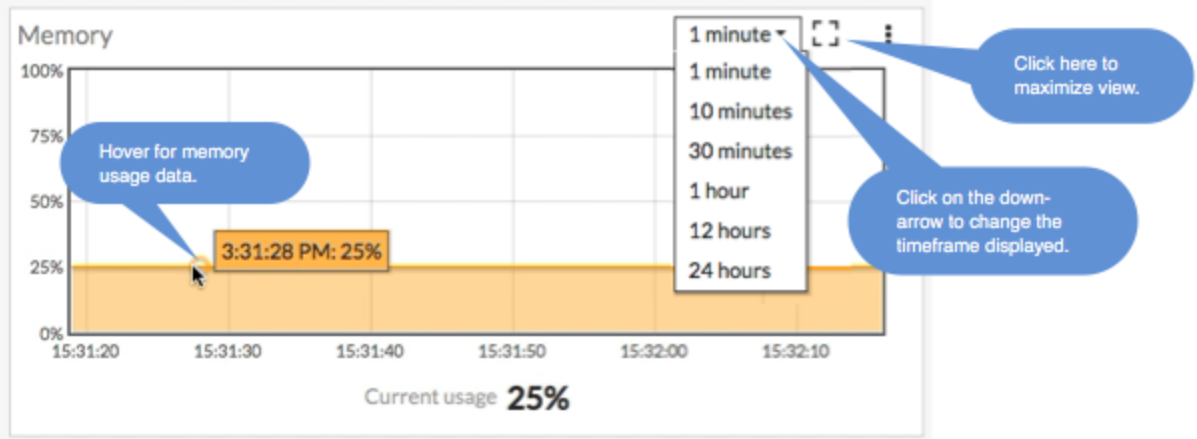
CPU

The real-time CPU usage is displayed for different time frames.

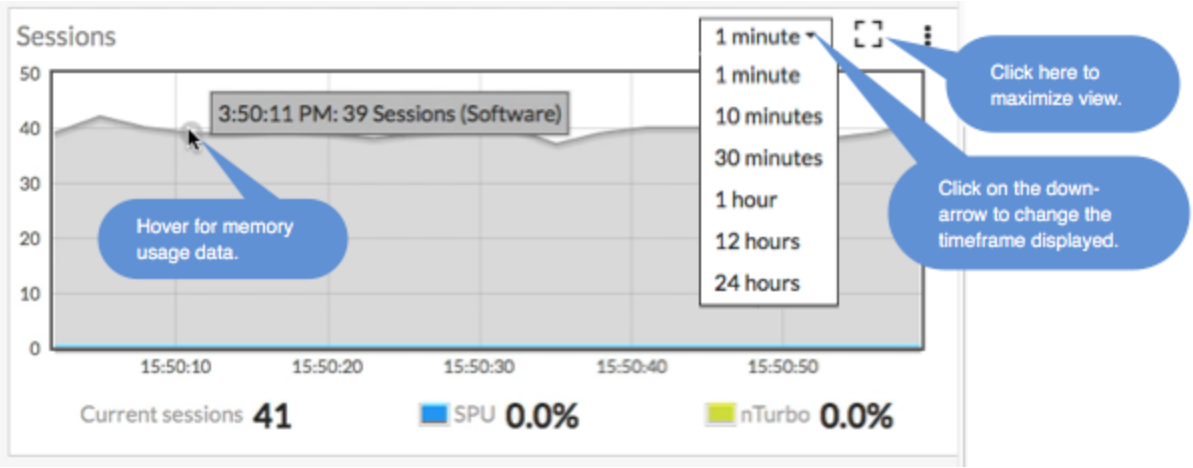


Memory

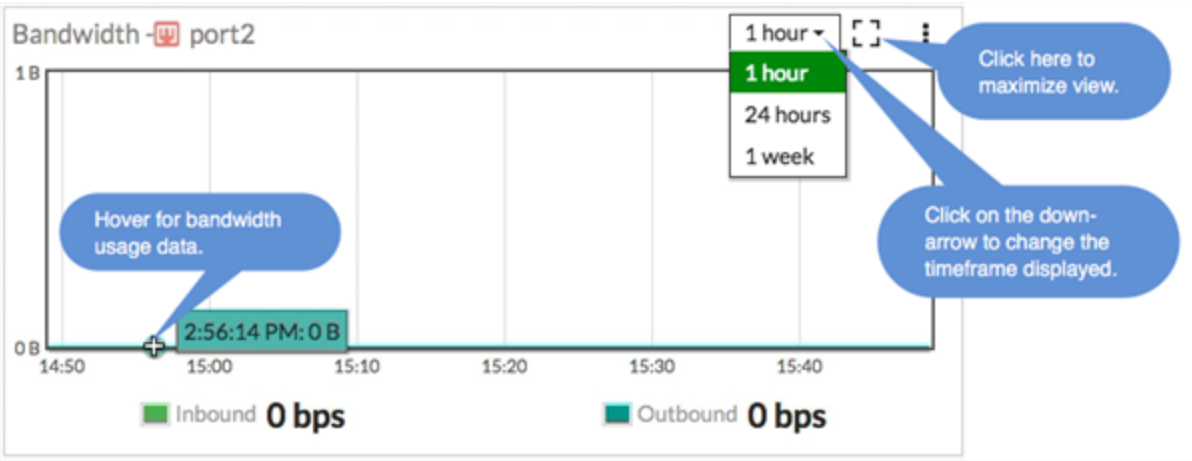
Real-time memory usage is displayed for different time frames. Hovering over any point on the graph displays percentage of memory used along with a timestamp.



Sessions



Bandwidth



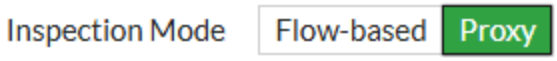
Two new policy modes are available in FortiOS 5.6.

- NGFW policy mode simplifies applying application control and web filtering to traffic by allowing you to add applications and web filtering categories directly to policies.
- Transparent proxy mode allows you to apply web authentication to HTTP traffic without using the explicit proxy.

Setting up the FortiGate to operate in these new modes (or to operate in the other available operating modes) involves going to **System > Settings** and changing the **Inspection** and **NGFW** modes.

Changing inspection modes (flow-based or proxy-based)

To change inspection modes, go to **System > Settings** and scroll down to **Inspection Mode**. You can select Flow-based to operate in Flow mode or Proxy to operate in Proxy mode. Flow-based inspection is the default inspection mode for FortiOS 5.6.



Transparent Web proxy mode

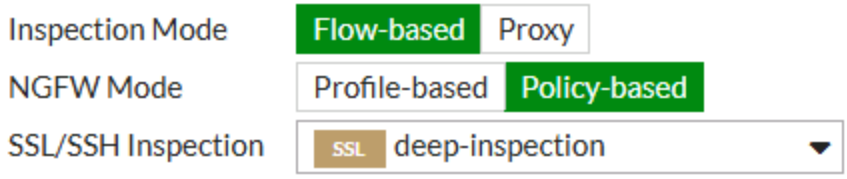
In proxy mode, FortiOS 5.6 functions just like FortiOS 5.4 with the addition of the new Transparent Web Proxy mode. See New Operating mode for Transparent web proxy (386474) on page 1.

NGFW profile-based and NGFW policy-based modes

When you use **Flow-based** as the **Inspection Mode**, you have the option in FortiOS 5.6 to select an **NGFW Mode**. **Profile-based** mode works the same as flow-based mode did in FortiOS 5.4

Flow-based inspection with profile-based **NGFW mode** is the default in FortiOS 5.6.

In the new **NGFW Policy-based** mode, you add applications and web filtering profiles directly to a policy without having to first create and configure Application Control or Web Filtering profiles. When selecting NGFW policy-based mode you can also select the SSL/SSH Inspection mode that is applied to all policies. See NGFW Policy Mode (371602) on page 1.



When you use flow-based inspection, all proxy mode profiles are converted to flow mode, removing any proxy settings. And proxy-mode only features (for example, Web Application Profile) are removed from the GUI.

If your FortiGate has multiple VDOMs, you can set the inspection mode independently for each VDOM. Go to **System > VDOM**. Click **Edit** for the VDOM you wish to change and select the **Inspection Mode**.

CLI syntax

The following CLI commands can be used to configure inspection and policy modes:

```
config system settings
   set inspection-mode {proxy | flow}
   set policy-mode {standard | ngfw}
end
```

Change to CLI console (396225)

The CLI Console widget has been removed from FortiOS 5.6.0. It is accessed from the upper-right hand corner of the screen and is no longer a pop-out window but a sliding window.

System Information Dashboard widget WAN IP Information enhancement (401464)

WAN IP and location data are now available in the **System Information** widget. Additionally, If the WAN IP is blacklisted in the FortiGuard server, there will be a notification in the notification area, located in the upper right-hand corner of the **Dashboard**. Clicking on the notification will open the WAN IP Blacklisted slider with the relevant blacklist information.

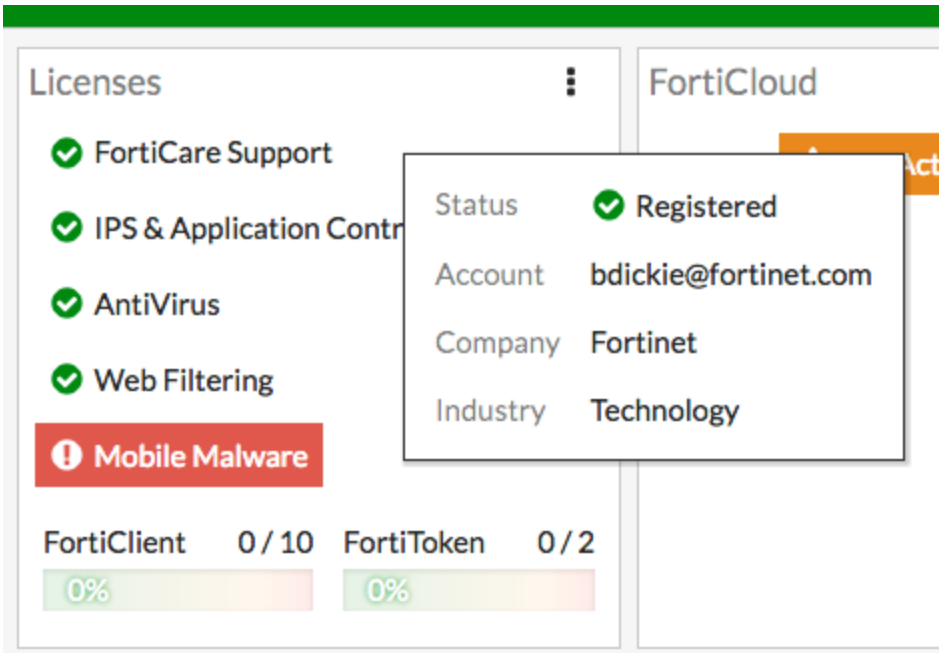
CLI and GUI changes to display FortiCare registration information (395254)

The changes pertain to industry and organization size of the FortiGate's registered owner.

GUI Changes

- Add industry and organization size to FortiCare registration page
- Add company and industry to license widget tooltip for FortiCare

When you hover over the Licenses widget in the FortiOS 5.6 dashboard, you can see the company and industry data, provided it has been entered in the FortiCare profile.



CLI Changes

Commands are added to `diagnose forticare`

```
dia forticare direct-registration product-registration -h
Options: a:A:y:C:c:T:eF:f:hI:i:l:O:o:p:P:z:R:r:S:s:t:v:
   --&lt;long&gt; -&lt;short&gt;
   account_id a:
   address A:
   city y:
   company C:
   contract_number c:
   country_code T:
   existing_account e
   fax F:
   first_name f:
   help h
   industry I:
   industry_id i:
   last_name l:
   orgsize O:
   orgsize_id o:
   password p:
   phone P:
   postal_code z:
   reseller R:
   reseller_id r:
   state S:
   state_code s:
   title t:
   version v:
```

Improved GUI for Mobile Screen Size & Touch Interface (355558)

The FortiOS web GUI on mobile screens and include functionality for touch interfaces like tap to hold are improved.

Installation

This section discusses how to install your FortiGate and use it in your network, after completion of the initial set-up outlined in the FortiGate model's Quick Start Guide. The section also provides troubleshooting tips.

The following topics are included in this section:

Setup Wizard

The Setup Wizard helps to quickly configure your FortiGate to allow Internet access and remote access. The wizard can be launched from the GUI by selecting the button, located in the top right corner (some entry-level models do not have this button). You can also get to the Setup Wizard through FortiExplorer which can be downloaded for either Windows or Mac OS at www.fortinet.com. FortiExplorer for iOS will be available through the App Store sometime in April 2017. See the What's New section for details.

More information on connecting to the GUI with FortiExplorer is found in the Using the GUI section.

Using the Setup Wizard

The Setup Wizard is intended to be used for initial setup. If it is used on a previously configured FortiGate, it replaces parts of the configuration, including existing firewall policies.

1. Connect to the FortiGate using FortiExplorer. View FortiExplorer in full-screen mode because some options may not be visible otherwise.
2. Select your FortiGate, then select **Setup Wizard**.
3. Login using an admin account (the default admin account has the username `admin` and no password).
4. Select **Change Password** to set a new password for the admin account. Select **Next**.
5. Select the appropriate time zone. Select **Next**.
6. Fill in the appropriate information about your **Internet WAN Connection**. Select **Next**.
7. Enter an **IP Address** and **Netmask** for your LAN. If necessary, enable **DHCP** and select a **Start** and **End Address**. Select **Next**.
8. Select the schedule for when Internet access should be allowed. Select **Next**.
9. Select the appropriate options for your **Internet Access Policy**, including **NAT** options and **Unified Threat Management**. Select **Next**.
10. If necessary, configure options to allow **Remote VPN Access** using either an SSL VPN or an IPsec VPN. Select **Next**.
11. A summary screen will appear. If the configuration shown is correct, select **Configure**.
12. (Optional) If you wish to activate a FortiCloud account, select **Next** and enter your information (for more information about FortiCloud, see the FortiCloud FAQ). Otherwise, select **Done**.

Results

Your configuration has now been set up on the FortiGate allowing users on the LAN to have Internet access.

Quick installation using DHCP

Most of the FortiGate desktop models have a default configuration that includes a DHCP server on the **lan** (or **internal**) interface and a security policy that securely allows all sessions from the Internal network to reach the Internet. Because of this, you can connect your desktop FortiGate to the Internet in two simple steps.

In order to use this installation method, your ISP must provide connectivity with DHCP and accept DHCP requests without authentication. You must also be using IPv4 to connect your FortiGate to the Internet.

1. Connect the FortiGate's **wan** interface to your ISP-supplied equipment, and then connect the internal network to the FortiGate's default **lan** interface. Turn on the ISP's equipment, the FortiGate, and the PCs on the internal network.
2. (Windows Vista/7/8/10 users) Go to **Network and Sharing Center** and select **Local Area Connections**. Select **Properties**. Select **Internet Protocol Version 4 (TCP/IPv4)**, then select **Properties**. Select **Obtain an IP address automatically** and **Obtain DNS server address automatically**.

   (Mac OS X users) Go to **System Preferences > Network** and select **Ethernet**. Set **Configure IPv4 to Using DHCP**.

Results

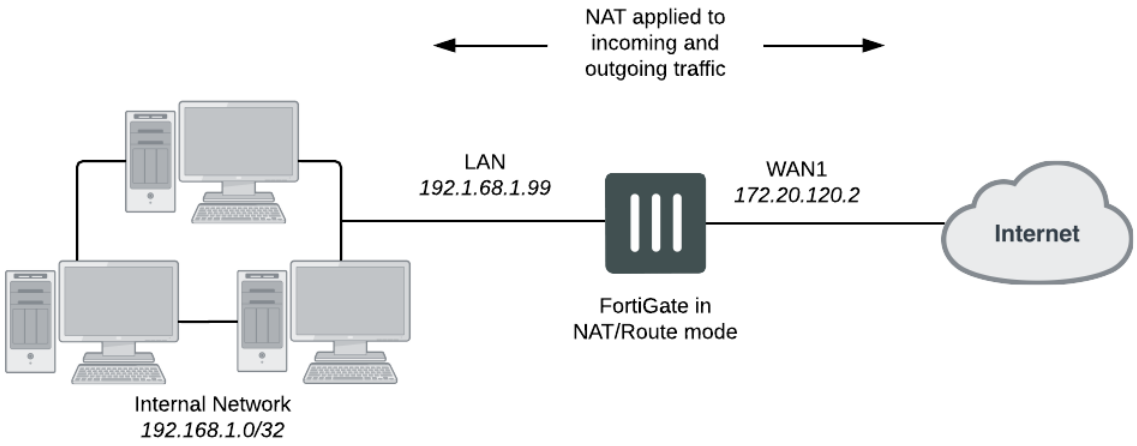
From any PC on the internal network, open a web browser and browse to any website. You can successfully connect to the Internet.

Installing a FortiGate in NAT/Route mode

There are two main ways to install a FortiGate using network address translation (NAT)/Route mode: Standard Installation in NAT/Route Mode, where Internet access is provided by a single ISP, and Redundant Internet Installation, where two ISPs are used.

Standard Installation in NAT/Route Mode

In this configuration, a FortiGate is installed as a gateway or router between a private network and the Internet. By using NAT, the FortiGate is able to hide the IP addresses of the private network.



Installing a FortiGate in NAT/Route Mode

1. Connect the FortiGate's Internet-facing interface (typically WAN or WAN1) to your ISP-supplied equipment.
2. Connect a PC to the FortiGate using an internal port (typically port 1).
3. Power on the ISP's equipment, the FortiGate, and the PC on the internal network.
4. From the PC on the internal network, connect to the FortiGate's GUI using either FortiExplorer or an Internet browser (for information about connecting to the GUI, please see your model's QuickStart Guide). Login using an admin account (the default admin account has the username `admin` and no password).
5. Go to **Network > Interfaces** and edit the Internet-facing interface. Set **Role**to **WAN** and set the **Estimated Bandwidth/Netmask** using Kbps.

If your FortiGate is directly connected to your ISP, set **Addressing Mode** to **Manual** and set the **IP/Netmask** to the private IP address you wish to use for the FortiGate.

If you have ISP equipment between your FortiGate and the Internet (for example, a router), then the wan1 IP will also use a private IP assigned by the ISP equipment. If this equipment uses DHCP, set **Addressing Mode** to **DHCP** to get an IP assigned to the interface.

If the ISP equipment does not use DHCP, your ISP can provide you with the correct private IP to use for the interface.

6. Edit the **lan** interface (called **internal** on some FortiGate models). Make sure the interface's **Role** is set to **LAN**. If you need your FortiGate to provide IP addresses to devices that connect to it, enable **DHCP Server**.
7. Go to **Network > Static Routes** and select **Create New** to add a default route. Set **Destination** to **Subnet**, which allows you to input a numeric IP address or subnet. Set **Destination IP/Mask** to 0.0.0.0/0.0.0.0, **Device** to the Internet-facing interface, and **Gateway** to the gateway (or default route) provided by your ISP or to the next hop router, depending on your network requirements.

A default route always has a Destination IP/Mask of 0.0.0.0/0.0.0.0. Normally, you would have only one default route. If the static route list already contains a default route, you can either edit it or delete it and add a new one.

8. (Optional) The FortiGate's DNS Settings are set to use FortiGuard DNS servers by default, which is sufficient for most networks. However, if you need to change the DNS servers, go to **Network > DNS**, select **Specify**, and add **Primary** and **Secondary** DNS servers.

Some FortiGate models include an IPv4 security policy allowing access from **LAN/Internal** to **WAN/WAN1** in the default configuration. This policy can be found at **Policy & Objects > IPv4 Policy**.

If you have one of these models, users are now able to access the Internet.

9. Go to **Policy & Objects > IPv4 Policy** and select **Create New** to add a security policy that allows users on the private network to access the Internet. Give the policy a Name that indicates that the policy will be for traffic to the Internet.

If your network uses IPv6 addresses, go to **Policy & Objects > IPv6 Policy** and select **Create New** to add a security policy that allows users on the private network to access the Internet. If the IPv6 menu option is not available, go to **System > Feature Select**, turn on **IPv6**, and select **Apply**. For more information on IPv6 networks, see the IPv6 Chapter of the Handbook.

10. In the policy, set the **Incoming Interface** to **lan** and the **Outgoing Interface** to the Internet-facing interface. You will also need to set **Source**, **Destination Address**, **Schedule**, and **Service** according to your network requirements. You can set these fields to the default all/ANY settings for now but should create the appropriate objects later after the policies have been verified. Make sure the **Action** is set to **ACCEPT**. Enable **NAT** and make sure **Use Outgoing Interface Address** is selected.

It is recommended to avoid using any security profiles, such as AntiVirus or Web Filter, until after you have successfully installed the FortiGate. After the installation is verified, you can apply any required security profiles.

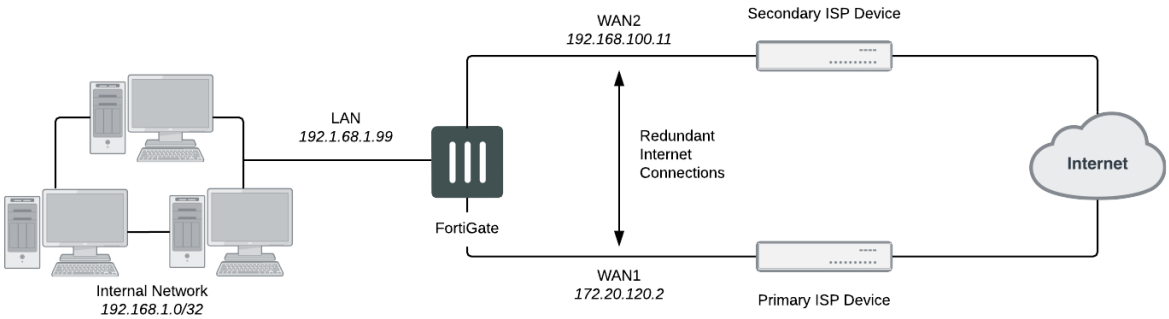
For more information about using security profiles, see the Security Profiles chapter of the Handbook.

Results

Users on the internal network are now able to access the Internet. They should also be able to connect to the Internet using any other protocol or connection method that you defined in the security policy.

Redundant Internet Installation

In this configuration, a WAN link interface is created providing the FortiGate with redundant Internet connections from two Internet service providers (ISPs). The WAN link interface combines these two connections, allowing the FortiGate to treat them as a single interface.



Installing a FortiGate with Redundant Internet

If you have previously configured your FortiGate using the standard installation, you will have to delete all routes and policies referring to an interface that will be used to provide redundant Internet. This includes the default Internet access policy that is included on many FortiGate models.

1. Connect your ISP devices to your FortiGate's Internet-facing interfaces (typically WAN1 and WAN2).
2. Go to **Network > SD-WAN** to create a WAN link interface, which is used to group multiple Internet connections together so that the FortiGate can treat them as a single interface.
3. Set the **Interface State** to **Enable**.
4. Under **SD-WAN**, select **Create New**. Add WAN1 and enter the Gateway IP provided by your primary ISP. Do the same for WAN2, but use the Gateway IP provided by your secondary ISP.
5. Select an appropriate method for the **Load Balancing Algorithm** from the following options:
   - **Volume** - A volume ratio is set for each active member of the SD-WAN link.
   - **Sessions** - A sessions ratio is set for each active member of the SD-WAN link.
   - **Spillover** - A traffic cap is defined for active members; when it is exceeded, the traffic will automatically activate the standby link.
   - **Source-Destination IP** - The next hop is based on both the traffic's source and destination IP address.
   - **Source IP based** - The next hop is based on the traffic's source IP address.
4. Add your Internet-facing interfaces to the WAN link interface and configure load balancing as required for each interface.
5. Go to **Network > Static Routes** and create a new default route. Set **Device** to the SD-WAN link.
6. Go to **Policy & Objects > IPv4 Policy** and select **Create New** to add a security policy that allows users on the private network to access the Internet.

If your network uses IPv6 addresses, go to **Policy & Objects > IPv6 Policy** and select **Create New** to add a security policy that allows users on the private network to access the Internet. If the IPv6 menu option is not available, go to **System > Feature Select**, turn on **IPv6**, and select **Apply**. For more information on IPv6 networks, see the IPv6 Handbook.

4. In the policy, set the **Incoming Interface** to the internal interface and the **Outgoing Interface** to the SD-WAN link interface. You will also need to set **Source Address**, **Destination Address**, **Schedule**, and **Service** according to your network requirements. You can set these fields to the default all/ANY settings for now but should create the appropriate objects later after the policies have been verified.
5. Make sure the **Action** is set to **ACCEPT**. Enable **NAT** and make sure **Use Destination Interface Address** is selected. Select **OK**.

It is recommended to avoid using any security profiles, such as AntiVirus or Web Filter, until after you have successfully installed the FortiGate. After the installation is verified, you can apply any required security profiles.

For more information about using security profiles, see the Security Profiles handbook.

Results

Users on the internal network are now able to browse the Internet. They should also be able to connect to the Internet using any other protocol or connection method defined in the security policy.

The amount of traffic an individual member of the SD-WAN link interface will use depends on the load balancing algorithm selected. You can view this usage by going to **FortiView > All Sessions** and viewing the **Destination Interface** column. If this column is not shown, right-click on the title row and select **Destination Interface** from the dropdown menu. Scroll to the bottom of the menu and select **Apply**.

NAT/Route Mode vs. Transparent Mode

A FortiGate can operate in one of two modes: NAT/Route or Transparent.

The most common of the two operating modes is NAT/Route mode, where a FortiGate is installed as a gateway or router between two networks. In most cases, it is used between a private network and the Internet. This allows the FortiGate to hide the IP addresses of the private network using network address translation (NAT). NAT/Route mode is also used when two or more Internet service providers (ISPs) provide the FortiGate with redundant Internet connections.

A FortiGate in Transparent mode is installed between the internal network and the router. In this mode, the FortiGate does not make any changes to IP addresses and only applies security scanning to traffic. When a FortiGate is added to a network in Transparent mode, no network changes are required, except to provide the FortiGate with a management IP address. Transparent mode is used primarily when there is a need to increase network protection but changing the configuration of the network itself is impractical.

For more information about Transparent Mode, see the Transparent Mode handbook.

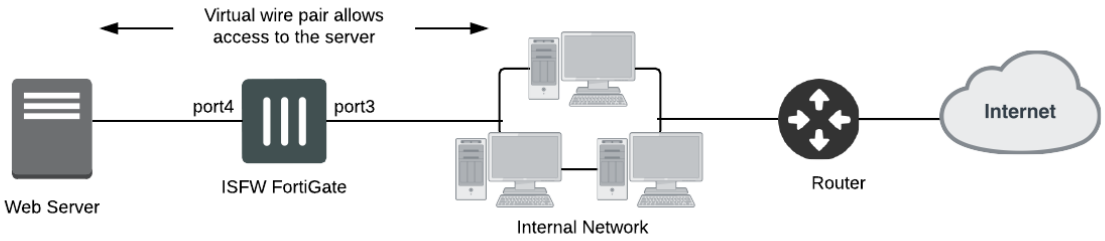
Using a Virtual Wire Pair

A virtual wire pair consists of two interfaces that have no IP addressing and are treated similar to a transparent mode VDOM. All traffic received by one interface in the virtual wire pair can only be forwarded out the other interface, provided that a virtual wire pair firewall policy allows this traffic. Traffic from other interfaces cannot be routed to the interfaces in a virtual wire pair.

Virtual wire pairs are useful for unusual topologies where MAC addresses do not behave normally: for example, port pairing can be used in a Direct Server Return (DSR) topology where the response MAC address pair may not match the request's MAC address pair.

In FortiOS 5.4, virtual wire pairing replaced the port pairing feature available in earlier firmware versions. Unlike port pairing, virtual wire pairing can be used for FortiGates in both NAT/Route and Transparent modes.

In the example configuration below, a virtual wire pair (consisting of port3 and port4) makes it easier to protect a web server that is behind a FortiGate operating as an Internal Segmentation Firewall (ISFW). Users on the internal network will access the web server through the ISFW over the virtual wire pair.



Adding a virtual wire pair and virtual wire pair policy

Interfaces used in a virtual wire pair cannot be used to access the ISFW FortiGate. Before creating a virtual wire pair, make sure you have a different port configured to allow admin access using your preferred protocol.

1. Go to **Network > Interfaces** and select **Create New > Virtual Wire Pair**.
2. Select the interfaces to add to the virtual wire pair. These interfaces cannot be part of a switch, such as the default **lan/internal** interface.
3. (Optional) If desired, enable **Wildcard VLAN**.
4. Select **OK**.
5. Go to **Policy & Objects > IPv4 Virtual Wire Pair Policy**, select the virtual wire pair, and select **Create New**.
6. Select the direction that traffic is allowed to flow.
7. Configure the other firewall options as desired.
8. Select **OK** .
9. If necessary, create a second virtual wire pair policy to allow traffic to flow in the opposite direction.

If you have a USB-wan interface, it will not be included in the interface list when building a wired-pair.

Results

Traffic can now flow through the FortiGate using the virtual wire pair.

For more information on this feature in FortiOS 5.6.0 , see the Firewall chapter.

Troubleshooting your FortiGate Installation

If your FortiGate does not function as desired after installation, try the following troubleshooting tips:

1. **Use FortiExplorer if you can't connect to the FortiGate over Ethernet.**
   If you can't connect to the FortiGate GUI or CLI, you may be able to connect using FortiExplorer. Refer to the QuickStart Guide or see the section on the FortiExplorer for more details.
2. **Check for equipment issues.**
   Verify that all network equipment is powered on and operating as expected. Refer to the QuickStart Guide for information about connecting your FortiGate to the network. You will also find detailed information about the FortiGate LED indicators.
3. **Check the physical network connections.**
   Check the cables used for all physical connections to ensure that they are fully connected and do not appear damaged, and make sure that each cable connects to the correct device and the correct Ethernet port on that device.
4. **Verify that you can connect to the internal IP address of the FortiGate.**
   Connect to the GUI from the FortiGate's internal interface by browsing to its IP address. From the PC, try to ping the internal interface IP address; for example, `ping 192.168.1.99`.
   If you cannot connect to the internal interface, verify the IP configuration of the PC. If you can ping the interface but can't connect to the GUI, check the settings for administrative access on that interface.
5. **Check the FortiGate interface configurations.**
   Check the configuration of the FortiGate interface connected to the internal network by going to **Network > Interfaces** and make sure **Addressing Mode** is set to the correct mode.
6. **Verify the security policy configuration.**
   Go to **Policy & Objects > IPv4 Policy** and verify that the internal interface to Internet-facing interface security policy has been added and is located near the top of the policy list. Check the **Active Sessions** column to ensure that traffic has been processed (if this column does not appear, right-click on the title row, select **Active Sessions**).
   If you are using NAT/Route mode, check the configuration of the policy to make sure that **NAT** is enabled and that **Use Outgoing Interface Address** is selected.
7. **Verify that you can connect to the Internet-facing interface's IP address.**
   Ping the IP address of the FortiGate's Internet-facing interface. If you cannot connect to the interface, the FortiGate is not allowing sessions from the internal interface to Internet-facing interface.
8. **Verify the static routing configuration.**
   Go to **Network > Static Routes** and verify that the default route is correct. Go to **Monitor > Routing Monitor** and verify that the default route appears in the list as a static route. Along with the default route, you should see two routes shown as **Connected**, one for each connected FortiGate interface.
9. **Verify that you can connect to the gateway provided by your ISP.**
   Ping the default gateway IP address from a PC on the internal network. If you cannot reach the gateway, contact your ISP to verify that you are using the correct gateway.
10. **Verify that you can communicate from the FortiGate to the Internet.**
    Access the FortiGate CLI and use the command `execute ping8.8.8.8`. You can also use the `execute traceroute 8.8.8.8` command to troubleshoot connectivity to the Internet.
11. **Verify the DNS configurations of the FortiGate and the PCs.**
    Check for DNS errors by pinging or using traceroute to connect to a domain name; for example: `ping www.fortinet.com`

If the name cannot be resolved, the FortiGate or PC cannot connect to a DNS server and you should confirm that the DNS server IP addresses are present and correct.

12. **Confirm that the FortiGate can connect to the FortiGuard network.**
    Once registered, the FortiGate obtains AntiVirus and Application Control and other updates from the FortiGuard network. Once the FortiGate is on your network, you should confirm that it can reach the FortiGuard network. First, check the **License Information** widget to make sure that the status of all FortiGuard services matches the services that you have purchased.
    Go to **System > FortiGuard**. Expand **Web Filtering and Email Filtering Options** and select **Test Availability**. After a minute, the GUI should indicate a successful connection.
13. **Consider changing the MAC address of your external interface.**
    Some ISPs do not want the MAC address of the device connecting to their network cable to change. If you have added a FortiGate to your network, you may have to change the MAC address of the Internet-facing interface using the following CLI command:

```
config system interface
   edit <interface>
      set macaddr <xx:xx:xx:xx:xx:xx>
   end
end
```

14. Either reset the FortiGate to factory defaults or contact Fortinet Support for assistance. See the note below before contacting support.
    To reset the FortiGate to factory defaults, use the CLI command `execute factoryreset`. When prompted, type `y` to confirm the reset.

You can also contact Fortinet Support for assistance. Read the following article found on the Fortinet Cookbook website: How to work with Fortinet Support to understand what type of support is available and to determine which level of support is right for you. For further information, go to support.fortinet.com.

Using the GUI

This section presents an introduction to the FortiGate's graphical user interface (GUI), also called the web-based manager.

The following topics are included in this section:

Connecting to the GUI

After completing your FortiGate's initial installation, there are two ways to connect to the GUI: using FortiExplorer or a web browser.

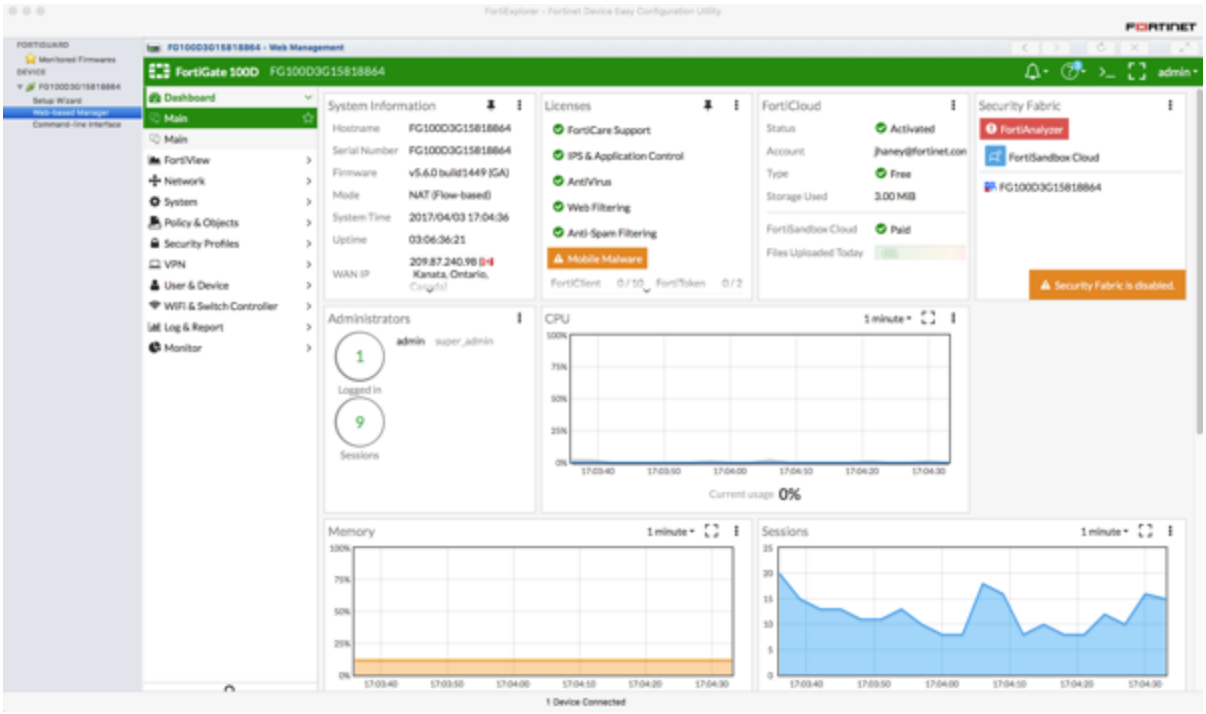
FortiExplorer

Connecting via your management computer

To connect to the GUI using FortiExplorer, connect your management computer to your FortiGate's USB management port, using the cable that came with the unit. FortiExplorer should open automatically once the devices are connected; if it does not, open the program manually.

To connect to the GUI, go to **Devices > Web-based Manager** and enter your username and password. If you have not changed the admin account's password, use the default user name, `admin`, and leave the password field blank.

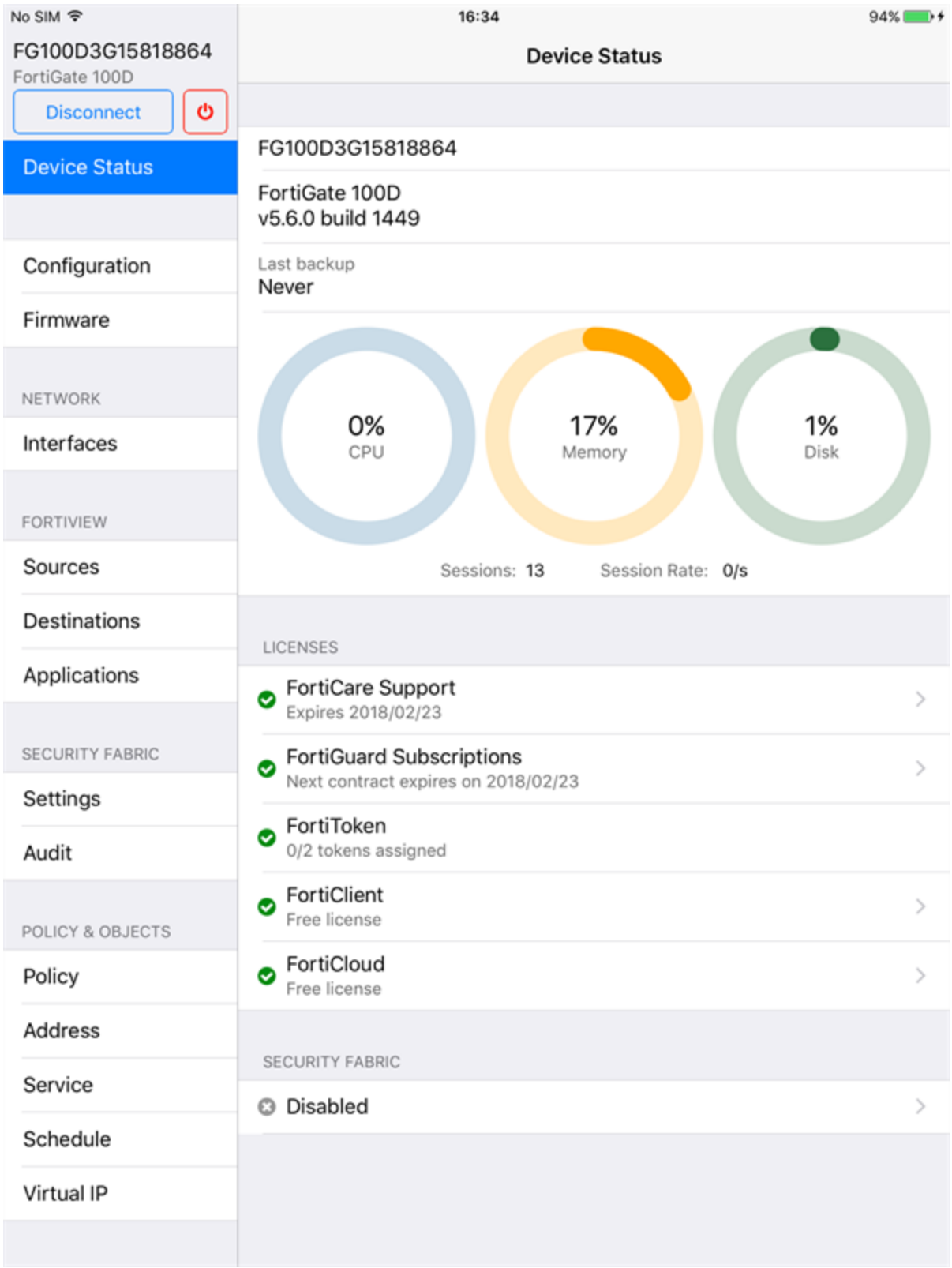
The GUI is now displayed in FortiExplorer.



Connecting via FortiExplorer for iOS

If you are using FortiExplorer for iOS, connect your iOS device to your FortiGate's USB management port. Open the FortiExplorer app and select your FortiGate from the list of **Devices**. Enter **USB** as the **Host** and then enter your username and password. If you have not changed the admin account's password, use the default user name, `admin`, and leave the password field blank.

The GUI is now displayed in FortiExplorer iOS.


No SIM
16:34
94%
FG100D3G15818864
FortiGate 100D
Disconnect
Device Status
Configuration
Firmware
NETWORK
Interfaces
FORTIVIEW
Sources
Destinations
Applications
SECURITY FABRIC
Settings
Audit
POLICY & OBJECTS
Policy
Address
Service
Schedule
Virtual IP
Device Status
FG100D3G15818864
FortiGate 100D
v5.6.0 build 1449
Last backup
Never
0%
CPU
17%
Memory
1%
Disk
Sessions: 13
Session Rate: 0/s
LICENSES
FortiCare Support
Expires 2018/02/23
FortiGuard Subscriptions
Next contract expires on 2018/02/23
FortiToken
0/2 tokens assigned
FortiClient
Free license
FortiCloud
Free license
SECURITY FABRIC
Disabled

Web browser

The recommended minimum screen resolution for properly displaying the GUI is 1280 by 1024. Check the FortiOS Release Notes for information about browser compatibility.

In order to connect to the GUI using a web browser, an interface must be configured to allow administrative access over HTTPS or over both HTTPS and HTTP. By default, an interface has already been set up that allows HTTPS access, with the IP address 192.168.1.99.

Browse to https://192.168.1.99 and enter your user name and password. If you have not changed the admin account's password, use the default user name, `admin`, and leave the password field blank.

The GUI will now be displayed in your browser.

If you wish to use a different interface to access the GUI, do the following:

1. Go to **Network > Interfaces** and edit the interface you wish to use for access. Take note of its assigned IP address.
2. Beside **Administrative Access**, select **HTTPS**. You can also select **HTTP**, although this is not recommended as the connection will be less secure.
3. Select **OK**.
4. Browse to the IP address using your chosen protocol.

Results

The GUI will now be displayed in your browser.

Menus

If there is a menu you believe your FortiGate model supports that does not appear in the GUI as expected, go to **System > Feature Select**and ensure the feature is enabled. For more information, see "Feature Select" on page 45.

The GUI contains the following main menus, which provide access to configuration options for most FortiOS features:

Dashboard	The dashboard displays various widgets that display important system information and allow you to configure some system options. For more information, see "Dashboard" on page 39.
FortiView	A collection of dashboards and logs that give insight into network traffic, showing which users are creating the most traffic, what sort of traffic it is, when the traffic occurs, and what kind of threat the traffic may pose to the network. For more information, see the FortiView chapter of the Handbook.
Network	Options for networking, including configuring system interfaces and routing options.
System	Configure system settings, such as administrators, FortiGuard, and certificates.
Policy & Objects	Configure firewall policies, protocol options, and supporting content for policies, including schedules, firewall addresses, and traffic shapers.
Security Profiles	Configure your FortiGate's security features, including AntiVirus, Web Filtering, and Application Control.
VPN	Configure options for IPsec and SSL virtual private networks (VPNs).
User & Device	Configure user accounts, groups, and authentication methods, including external authentication and single sign-on (SSO).
WiFi & Switch Controller	Configure the unit to act as a wireless network controller, managing the wireless Access Point (AP) functionality of FortiWiFi and FortiAP units. On certain FortiGate models, this menu has additional features allowing for FortiSwitch units to be managed by the FortiGate.
Log & Report	Configure logging and alert email as well as reports.

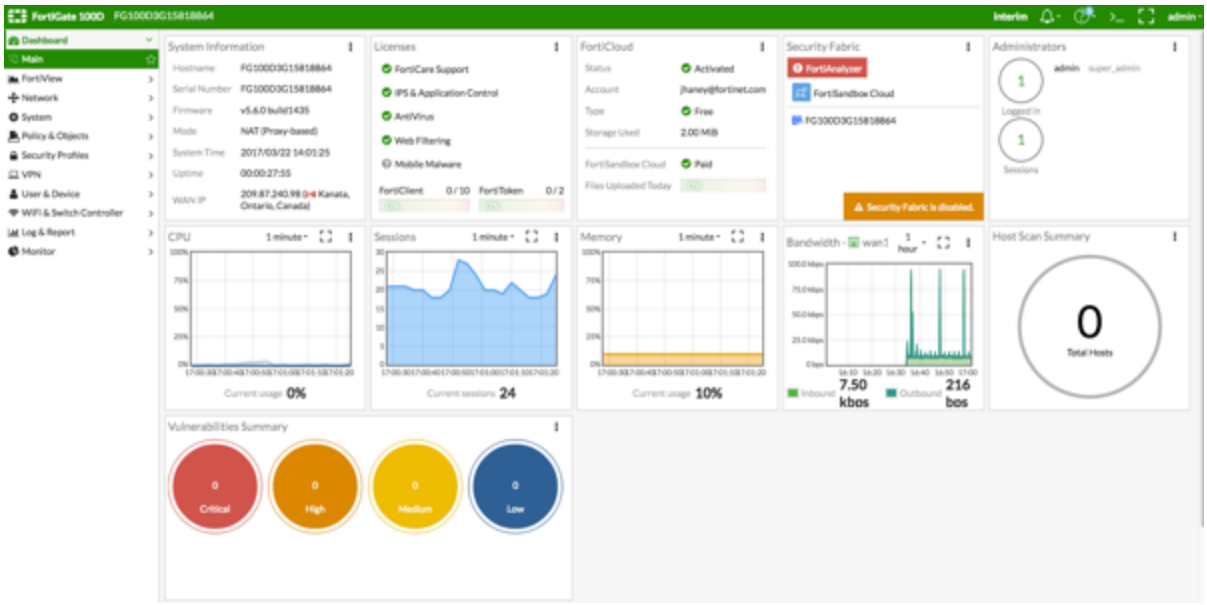
Monitor	View a variety of monitors, including the Routing Monitor, VPN monitors for both IPsec and SSL, and monitors relating to wireless networking.

Dashboard

The FortiOS 5.6 **Dashboard** has a new layout with a Network Operations Center (NOC) view with a focus on alerts. Widgets are interactive; by clicking or hovering over most widgets, the user can get additional information or follow links to other pages.

Enhancements to the GUI dashboard and its widgets are:

- Multiple dashboard support.
- VDOM and global dashboards.
- Updated resize control for widgets.
- Notifications moved to the top header bar (moved existing dashboard notifications to the header and added additional ones)..
- Reorganization of **Add Widget** dialog.
- New **Host Scan Summary** widget.
- New **Vulnerabilities Summary** widget that displays endpoint vulnerability information much like the FortiClient Enterprise Management Server (EMS) summary.
- Multiple bug fixes.



Features that were only visible through old dashboard widgets have been placed elsewhere in the GUI:

- Restore configuration.
- Configuration revisions.
- Firmware management.
- Enabling / disabling VDOMs.
- Changing inspection mode.
- Changing operation mode.

- Shutdown / restart device.
- Changing hostname.
- Changing system time.

The following **widgets are displayed by default**:

- System Information
- Licenses
- FortiCloud
- Security Fabric
- Administrators
- CPU
- Memory
- Sessions
- Bandwidth

The following **optional** widgets are available:

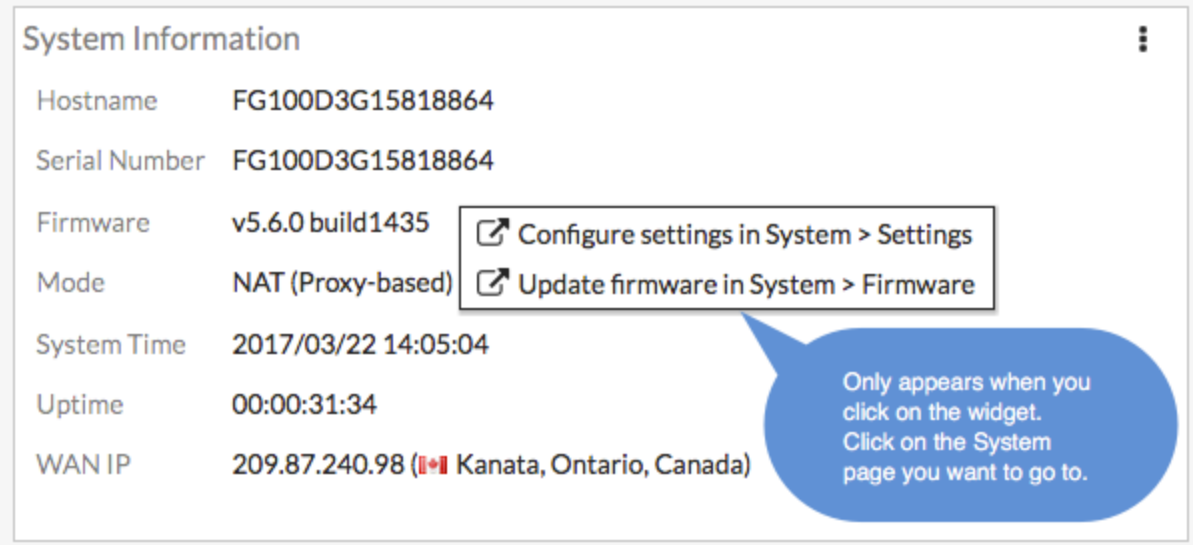
- Interface Bandwidth
- Disk Usage
- Security Fabric Risk
- Advanced Threat Protection Statistics
- Log Rate
- Session Rate
- Sensor Information
- HA Status
- Host Scan Summary
- Vulnerabilities Summary

The following widgets have been **removed**:

- CLI Console
- Unit Operation
- Alert Message Console

System Information

WAN IP and location data are now available in the **System Information** widget. Additionally, If the WAN IP is blacklisted in the FortiGuard server, there will be a notification in the notification area, located in the upper right-hand corner of the **Dashboard**. Clicking on the notification will open the WAN IP Blacklisted slider with the relevant blacklist information.

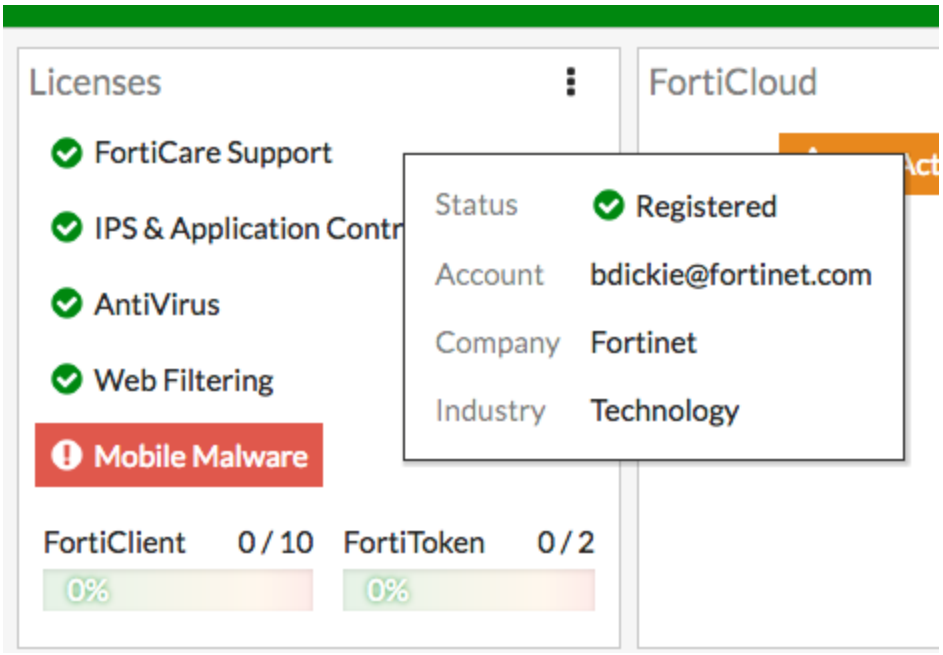


Licenses

Hovering over the **Licenses** widget will cause status information (and, where applicable, database information) on the licenses to be displayed for **FortiCare Support**, **IPS & Application Control**, **AntiVirus**, **Web Filtering**, **Mobile Malware**, and **FortiClient**.

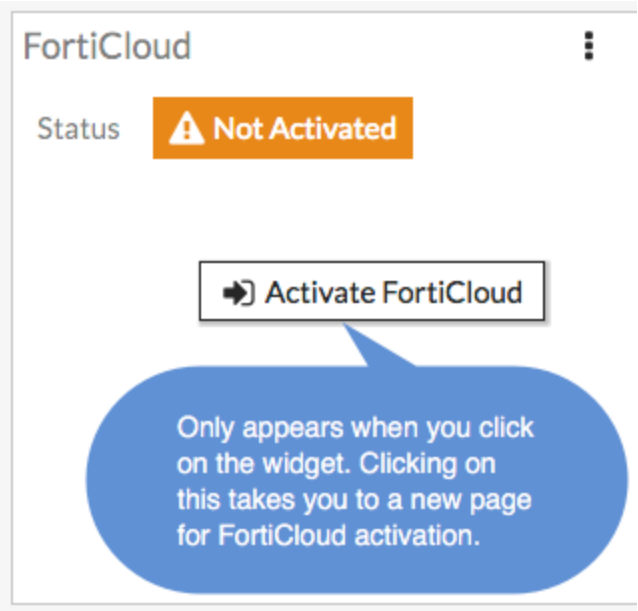
The image below shows **FortiCare Support** information along with the registrant's company name and industry, provided that information was entered in the FortiCare profile.

Clicking on different points in the **Licenses** widget will provide you with expiry dates on your licenses and links to other pages, such as **System > FortiGuard** or contract renewal pages.



FortiCloud

This widget displays FortiCloud status and provides a link to activate FortiCloud.

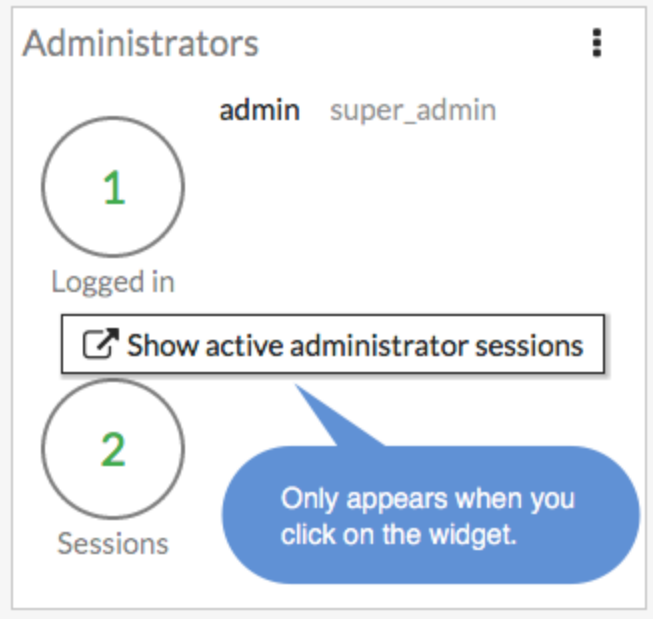


Security Fabric

The **Security Fabric** widget is documented in the Security Fabric section of the **What's New** document.

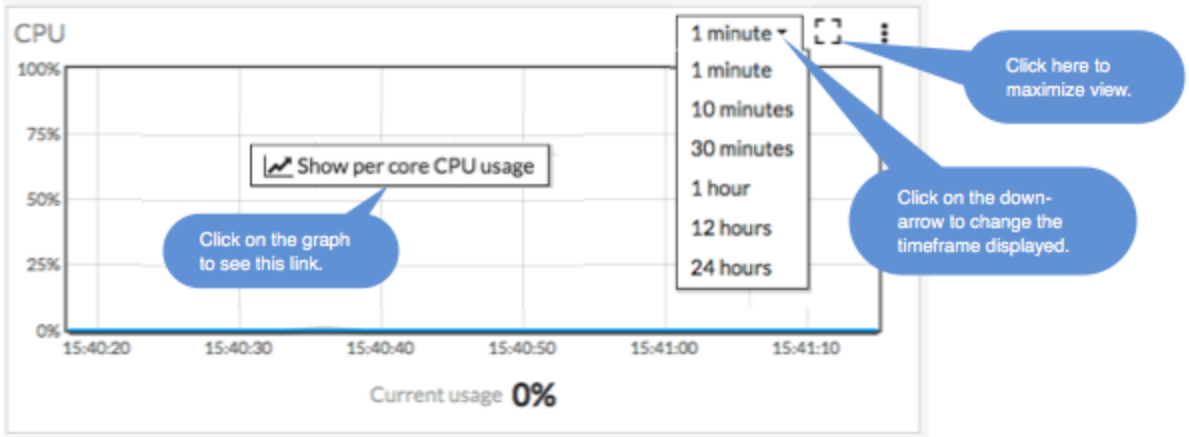
Administrators

This widget allows you to view which administrators are logged in and how many sessions are active. The link directs you to a page displaying active administrator sessions.



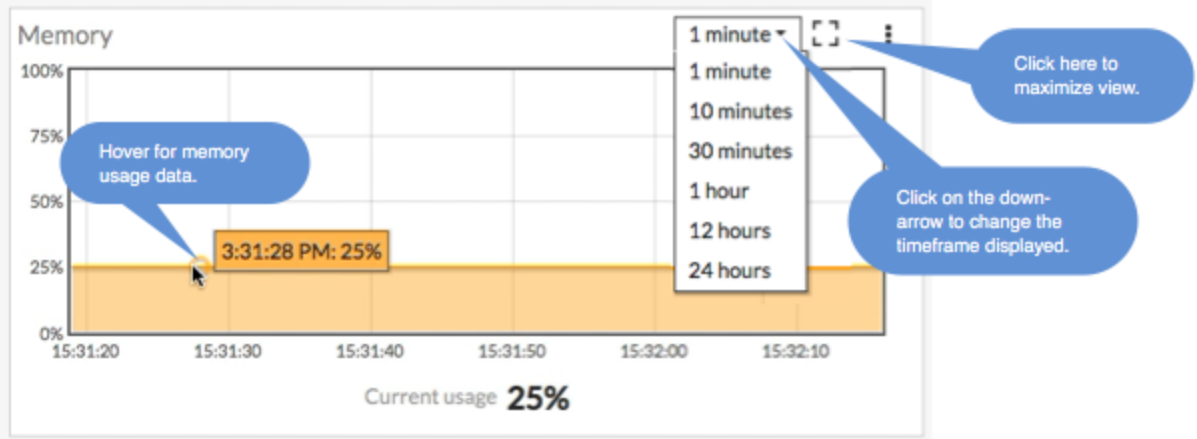
CPU

The real-time CPU usage is displayed for different time frames.

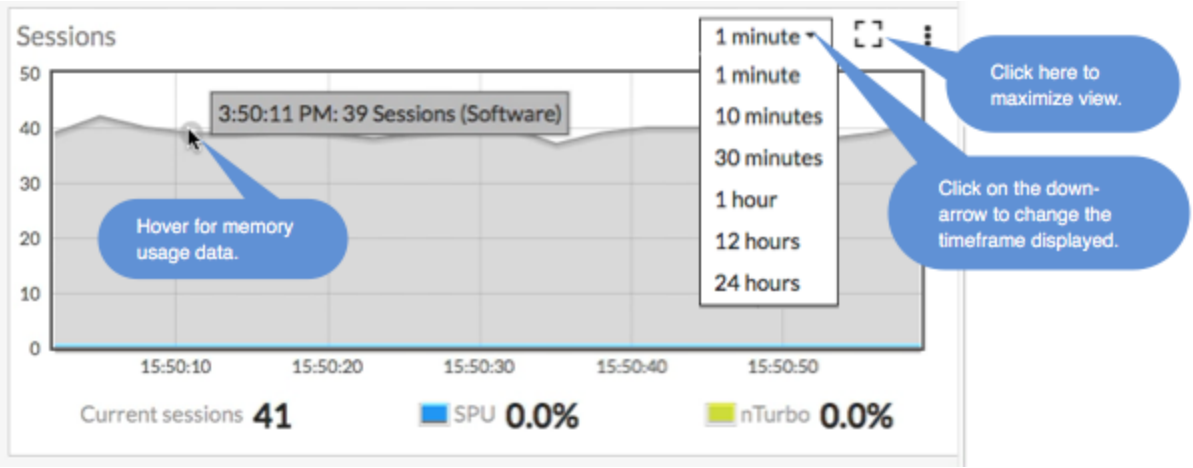


Memory

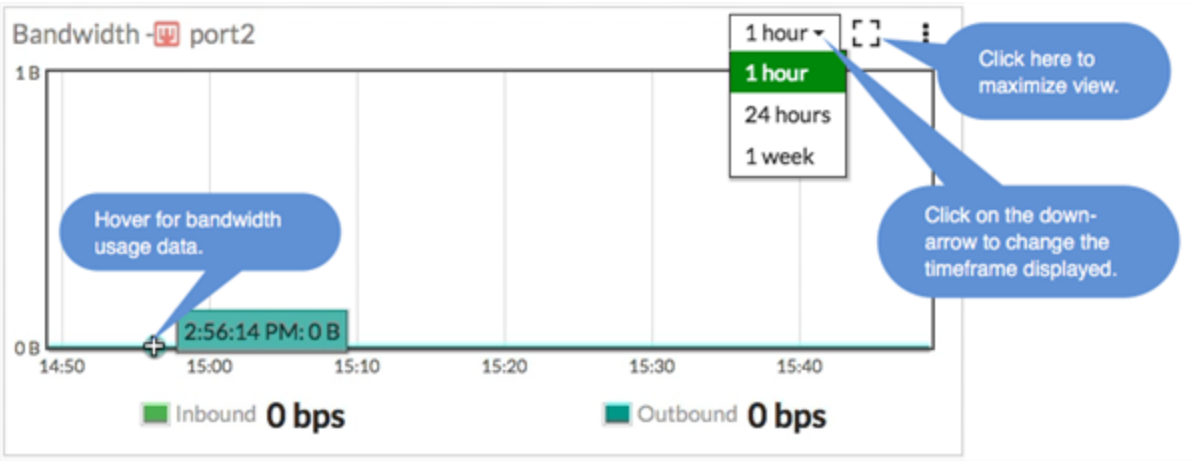
Real-time memory usage is displayed for different time frames. Hovering over any point on the graph displays percentage of memory used along with a timestamp.



Sessions



Bandwidth



Feature Select

Feature Select is used to control which features are visible in the GUI. This allows you to hide features that are not being used. Some features are also disabled by default and must be enabled in order to configure them through the GUI.

Feature Select only alters the visibility of these features, rather than their functionality. For example, disabling web filtering using Feature Select does not remove web filtering from the FortiGate, but removes the option of configuring web filtering from the GUI. Configuration options will still be available using the CLI.

Enabling / disabling features

Feature Select can be found at **System > Feature Select**. Once you have accessed Feature Select, ensure all features you wish to use are turned on, and that features you wish to hide are turned off. When you have finished, select **Apply**.

Security Features Presets

The main Security Features can be turned off individually or the five system presets can be used:

- **NGFW** should be chosen for networks that require application control and protection from external attacks.
- **ATP** should be chosen for networks that require protection from viruses and other external threats.
- **WF** should be chosen for networks that require web filtering.
- **NGFW + ATP** should be chosen for networks that require protection from external threats and attacks.
- **UTM** should be chosen for networks that require protection from external threats and wish to use security features that control network usage.
- **Full UTM** should be chosen for networks that require full protection from FortiOS. UTM is the default setting.

Tables

Many of the GUI pages contain tables of information that you can filter to display specific information. Administrators with read and write access can define the filters.

Navigation

Some tables contain information and lists that span multiple pages. At the bottom of the page are the page navigation controls.

Filters

Filters are used to locate a specific set of information or content within multiple pages. These are especially useful in locating specific log entries. The specific filtering options vary, depending on the type of information in the log.

To create a filter, select **Add Filter** at the top of the page. A list of the available fields for filtering will be shown.

Column settings

Column settings are used to select the types of information which are displayed on a certain page. Some pages have a large amounts of information is available and not all content can be displayed on a single screen. Also, some pages may contain content that is not of use to you. Using column settings, you can display only that content which is important to your requirements.

To configure column settings, right-click the header of a column and select the columns you wish to view and de-select any you wish to hide. After you have finished making your selections, select **Apply** (you may need to scroll down the list to do so).

Any changes that you make to the column settings of a list are stored in the unit's configuration and will display the next time that you access the list. To return a page's columns to the default state, select **Reset All Columns**, located at the bottom of the **Selected Columns** list.

Cloning objects

On some tables containing configuration objects, such as the policy table found at **Policy & Objects > IPv4 Policy**, you have the option of cloning an object on the table. This allows you to create a copy of that object, which you can then configure as needed. You can also reverse clone a policy to change the direction of the traffic impacted by that policy.

To clone an object, first select that object, then right-click to make a menu appear and select the **Copy** option. Then right-click the row in the table that is either above or below where you want the copied object to be placed, select the **Paste** option and indicate **Above** or **Below**.

Reverse cloning works much the same way. Instead of selecting Copy, you will select **Clone Reverse**.

Once the policy is copied, you must give it a name, configure as needed, and enable it.

Editing objects

Some tables allow you to edit parts of the configuration direction on the table's page. For example, security features can be added to an existing firewall policy from the policy list (**Policy & Objects > IPv4 Policy**), by clicking on the plus sign in the**Security Profiles** column and selecting the appropriate profiles.

If this option is not available, you must select the object, then open the policy by selecting the **Edit** option, found at the top of the page.

Text Strings

The configuration of a FortiGate is stored in the FortiOS configuration database. To change the configuration, you can use the GUI or CLI to add, delete, or change configuration settings. These changes are stored in the database as you make them.

Individual settings in the configuration database can be text strings, numeric values, selections from a list of allowed options, or on/off (enable/disable) settings.

Entering text strings (names)

Text strings are used to name entities in the configuration. For example, the name of a firewall address, administrative user, and so on. You can enter any character in a FortiGate configuration text string except, to prevent Cross-Site Scripting (XSS) vulnerabilities, the following characters:

" (double quote), & (ampersand), ' (single quote), < (less than) and > (greater than)

Most GUI text string fields make it easy to add an acceptable number of characters and prevent you from adding the XSS vulnerability characters.

There is a different character limitation for VDOM names and hostnames. For both, the only valid characters are numbers (0-9), letters (a-z, A-Z), and special characters - and _.

From the CLI, you can also use the `tree` command to view the number of characters that are allowed in a name field. For example, firewall address names can contain up to 64 characters. When you add a firewall address to the GUI, you are limited to entering 64 characters in the firewall address name field. From the CLI you can enter the following `tree` command to confirm that the firewall address `name` field allows 64 characters.

```
config firewall address
   tree
   -- [address] --*name (64)
   |- uuid
   |- subnet
   |- type
   |- start-ip
   |- end-ip
   |- fqdn (256)
   |- country (3)
   |- cache-ttl (0,86400)
   |- wildcard
   |- comment
   |- visibility
   |- associated-interface (36)
   |- color (0,32)
   |- [tags] --*name (65)
   +- allow-routing
```

The `tree` command output also shows the number of characters allowed for other firewall address name settings. For example, the fully-qualified domain name (`fqdn`) field can contain up to 256 characters.

Entering numeric values

Numeric values set various sizes, rates, numeric addresses, and other numeric values. For example, a static routing priority of 10, a port number of 8080, or an IP address of 10.10.10.1. Numeric values can be entered as a series of digits without spaces or commas (for example, 10 or 64400), in dotted decimal format (for example the IP address 10.10.10.1) or, as in the case of MAC or IPv6 addresses, separated by colons (for example, the MAC address 00:09:0F:B7:37:00). Most numeric values are standard base-10 numbers, but some fields (again, such as MAC addresses) require hexadecimal numbers.

Most GUI numeric value fields make it easy to add the acceptable number of digits within the allowed range. CLI help includes information about allowed numeric value ranges. Both the GUI and the CLI prevent you from entering invalid numbers.

Using the CLI

The command line interface (CLI) is an alternative configuration tool to the GUI or web-based manager. While the configuration of the GUI uses a point-and-click method, the CLI requires typing commands or uploading batches of commands from a text file, like a configuration script.

This section explains common CLI tasks that an administrator does on a regular basis and includes the topics:

Connecting to the CLI

You can access the CLI in three ways:

- Locally with a console cable — Connect your computer directly to the FortiGate unit's console port. Local access is required in some cases:
  - If you are installing your FortiGate unit for the first time and it is not yet configured to connect to your network, you may only be able to connect to the CLI using a local serial console connection, unless you reconfigure your computer's network settings for a peer connection.
  - Restoring the firmware utilizes a boot interrupt. Network access to the CLI is not available until after the boot process has completed, making local CLI access the only viable option.
- Through the network — Connect your computer through any network attached to one of the FortiGate unit's network ports. The network interface must have enabled Telnet or SSH administrative access if you will connect using an SSH/Telnet client, or HTTP/HTTPS administrative access if you will connect by accessing the **CLI Console** in the GUI. The CLI console widget is no longer part of the **Dashboard** with FortiOS 5.6. It can be accessed, however, from the upper-right hand corner of the screen and is no longer a pop-out window but a sliding window.
- Locally with FortiExplorer — Connect your computer directly to the FortiGate unit's USB management port. FortiExplorer provides direct access to the FortiOS setup wizard, Web-based Manager, and CLI console.

Connecting to the CLI using a local console

Local console connections to the CLI are formed by directly connecting your management computer or console to the FortiGate unit, using its DB-9 or RJ-45 console port. To connect to the local console you need:

- A computer with an available serial communications (COM) port.
- The RJ-45-to-DB-9 or null modem cable included in your FortiGate package.
- Terminal emulation software such as HyperTerminal for Microsoft Windows.

The following procedure describes connection using Microsoft HyperTerminal software; steps may vary with other terminal emulators.

To connect to the CLI using a local serial console connection

1. Using the null modem or RJ-45-to-DB-9 cable, connect the FortiGate unit's console port to the serial communications (COM) port on your management computer.
2. On your management computer, start HyperTerminal.
3. For the **Connection Description**, enter a **Name** for the connection, and select **OK**.
4. On the **Connect using** drop-down list box, select the communications (COM) port on your management computer you are using to connect to the FortiGate unit.
5. Select **OK**.
6. Select the following **Port** settings and select **OK**.

Bits per second	9600
Data bits	8
Parity	None
Stop bits	1
Flow control	None

7. Press **Enter** or **Return** on your keyboard to connect to the CLI.
8. Type a valid administrator account name (such as `admin`) and press Enter.
9. Type the password for that administrator account and press Enter. (In its default state, there is no password for the `admin` account.)

   The CLI displays the following text:

   ```
   Welcome!
   Type ? to list available commands.
   ```

   You can now enter CLI commands, including configuring access to the CLI through SSH or Telnet.

Enabling access to the CLI through the network (SSH or Telnet)

SSH or Telnet access to the CLI is accomplished by connecting your computer to the FortiGate unit using one of its RJ-45 network ports. You can either connect directly, using a peer connection between the two, or through any intermediary network.

If you do not want to use an SSH/Telnet client and you have access to the web-based manager, you can alternatively access the CLI through the network using the **CLI Console** widget in the web-based manager.

You must enable SSH and/or Telnet on the network interface associated with that physical network port. If your computer is not connected directly or through a switch, you must also configure the FortiGate unit with a static route to a router that can forward packets from the FortiGate unit to your computer. You can do this using either a local console connection or the web-based manager.

Requirements

- A computer with an available serial communications (COM) port and RJ-45 port
- Terminal emulation software such as HyperTerminal for Microsoft Windows

- The RJ-45-to-DB-9 or null modem cable included in your FortiGate package
- A network cable
- Prior configuration of the operating mode, network interface, and static route.

To enable SSH or Telnet access to the CLI using a local console connection

1. Using the network cable, connect the FortiGate unit's network port either directly to your computer's network port, or to a network through which your computer can reach the FortiGate unit.
2. Note the number of the physical network port.
3. Using a local console connection, connect and log into the CLI.
4. Enter the following command:

```
config system interface
   edit <interface_str>
      set allowaccess <protocols_list>
      end
```

   where:

   - `<interface_str>` is the name of the network interface associated with the physical network port and containing its number, such as `port1`
   - `<protocols_list>` is the complete, space-delimited list of permitted administrative access protocols, such as `https ssh telnet`

   For example, to exclude HTTP, HTTPS, SNMP, and PING, and allow only SSH and Telnet administrative access on `port1`:

```
config system interface
   edit port1
      set allowaccess ssh telnet
      end
```

5. To confirm the configuration, enter the command to display the network interface's settings.

```
show system interface <interface_str>
```

   The CLI displays the settings, including the allowed administrative access protocols, for the network interfaces.

Connecting to the CLI using SSH

Once the FortiGate unit is configured to accept SSH connections, you can use an SSH client on your management computer to connect to the CLI.

Secure Shell (SSH) provides both secure authentication and secure communications to the CLI. FortiGate units support 3DES and Blowfish encryption algorithms for SSH.

Before you can connect to the CLI using SSH, you must first configure a network interface to accept SSH connections. The following procedure uses PuTTY. Steps may vary with other SSH clients.

To connect to the CLI using SSH

1. On your management computer, start an SSH client.
2. In **Host Name (or IP Address)**, enter the IP address of a network interface on which you have enabled SSH administrative access.
3. In **Port**, enter `22`.

4. For the **Connection type**, select **SSH**.
5. Select **Open**.
   The SSH client connects to the FortiGate unit.

   The SSH client may display a warning if this is the first time you are connecting to the FortiGate unit and its SSH key is not yet recognized by your SSH client, or if you have previously connected to the FortiGate unit but used a different IP address or SSH key. This is normal If your management computer is directly connected to the FortiGate unit with no network hosts between them.
6. Click **Yes** to verify the fingerprint and accept the FortiGate unit's SSH key. You will not be able to log in until you have accepted the key.
7. The CLI displays a login prompt.
8. Type a valid administrator account name (such as `admin`) and press Enter.
9. Type the password for this administrator account and press Enter.
   The FortiGate unit displays a command prompt (its host name followed by a `#`. You can now enter CLI commands.

If three incorrect login or password attempts occur in a row, you will be disconnected. If this occurs, wait one minute, then reconnect to attempt the login again.

Connecting to the CLI using Telnet

Once the FortiGate unit is configured to accept Telnet connections, you can use a Telnet client on your management computer to connect to the CLI.

Telnet is not a secure access method. SSH should be used to access the CLI from the Internet or any other untrusted network.

Before you can connect to the CLI using Telnet, you must first configure a network interface to accept Telnet connections.

To connect to the CLI using Telnet

1. On your management computer, start a Telnet client.
2. Connect to a FortiGate network interface on which you have enabled Telnet.
3. Type a valid administrator account name (such as `admin`) and press Enter.
4. Type the password for this administrator account and press Enter.
   The FortiGate unit displays a command prompt (its host name followed by a `#`. You can now enter CLI commands.

If three incorrect login or password attempts occur in a row, you will be disconnected. If this occurs, wait one minute, then reconnect to attempt the login again.

Connecting to the CLI locally with FortiExplorer

FortiExplorer is a standalone software solution that allows you to connect to your FortiGate device using the USB interface of your management computer. FortiExplorer provides direct access to the FortiOS setup wizard, Web-based Manager, and CLI console.

FortiExplorer is available for download from the Customer Service & Support web site https://support.fortinet.com in firmware images. FortiExplorer is available for both Microsoft Windows and Mac OS X computers.

FortiExplorer provides a user-friendly tool that you can use to configure a FortiGate unit over a standard USB connection, rather than using a console cable or Ethernet connection.

Do not connect the USB cable until after FortiExplorer has been installed.

Installing FortiExplorer on Microsoft Windows

To install FortiExplorer on a Microsoft Windows workstation:

1. Double-click the .msi or .exe file and follow the instructions on-screen.
2. Connect the USB cable to the FortiGate unit and then to the management computer.
3. The FortiExplorer Fortinet Device Easy Configuration Utility opens when the USB cable is connected. Select ***Install the hardware automatically*** and select ***Next***.
4. After a moment, FortiExplorer will launch.

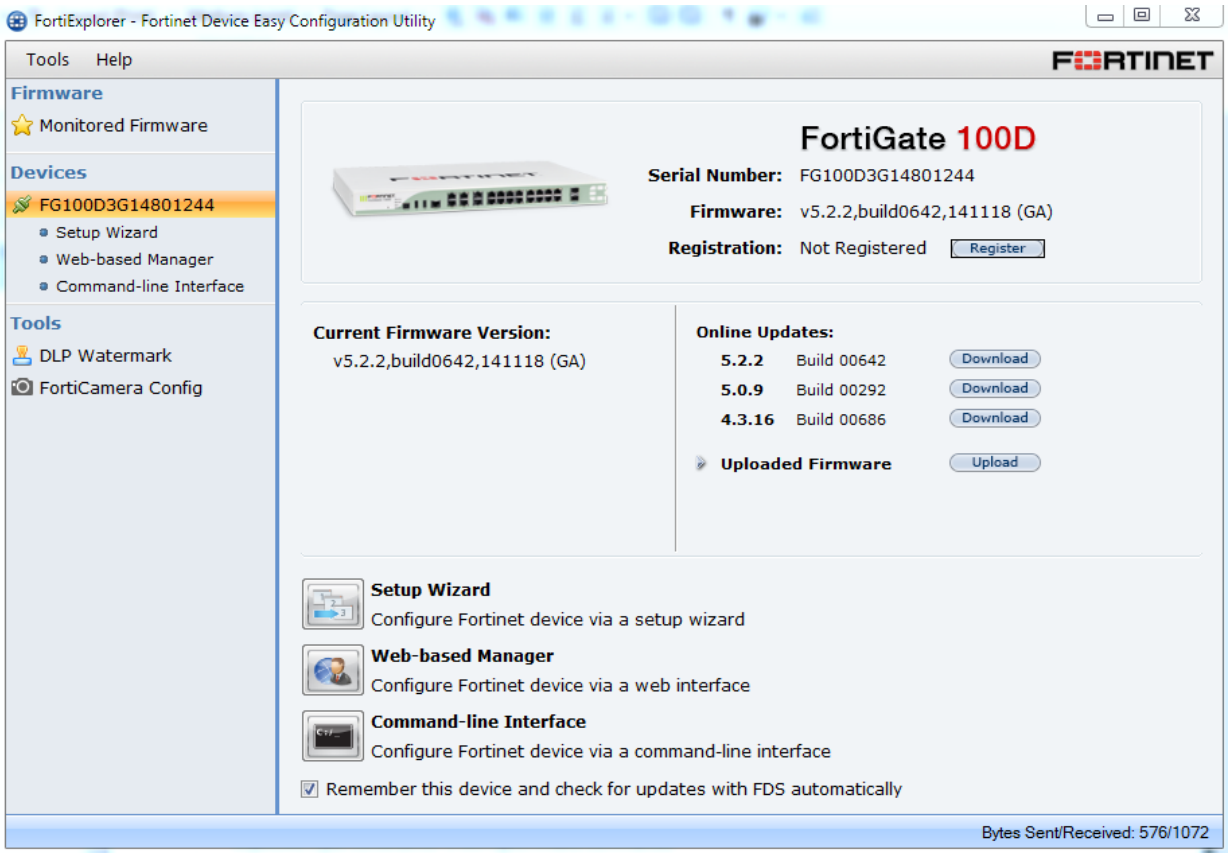
Installing FortiExplorer on Mac OS X

To install FortiExplorer on a Mac OS X workstation:

1. Double-click the .dmg file and drag the FortiExplorer program file into the Applications folder.
2. Connect the USB cable to the FortiGate unit and then to the management computer.
3. Double-click the FortiExplorer icon to launch the application.

Starting the CLI from FortiExplorer

The below image shows the FortiExplorer tool connected to a FortiGate 100D device, under ***Devices***, click on ***Command-line Interface*** and you will be connected to the CLI:


FortiExplorer - Fortinet Device Easy Configuration Utility
Tools
Help
FORTINET
Firmware
Monitored Firmware
Devices
FG100D3G14801244
Setup Wizard
Web-based Manager
Command-line Interface
Tools
DLP Watermark
FortiCamera Config
FortiGate 100D
Serial Number: FG100D3G14801244
Firmware: v5.2.2,build0642,141118 (GA)
Registration: Not Registered
Register
Current Firmware Version:
v5.2.2,build0642,141118 (GA)
Online Updates:
5.2.2 Build 00642 Download
5.0.9 Build 00292 Download
4.3.16 Build 00686 Download
Uploaded Firmware Upload
Setup Wizard
Configure Fortinet device via a setup wizard
Web-based Manager
Configure Fortinet device via a web interface
Command-line Interface
Configure Fortinet device via a command-line interface
Remember this device and check for updates with FDS automatically
Bytes Sent/Received: 576/1072

CLI-only features

As you can see in the Feature / Platform Matrix, the entry level models have a number of features that are only available using the Command Line Interface (CLI), rather than appearing in the GUI.

You can use FortiExplorer or terminal emulation software to access the CLI. The CLI Console can also be accessed by going to the **Dashboard** and using the drop-down menu at the top right corner of the page.

You can also open the CLI console so that it automatically opens to the object you wish to configure. For example, to edit a firewall policy, right-click on the policy in the policy list (**Policy & Objects > IPv4 Policy**) and select **Edit in CLI**. The CLI console will appear, with the commands to access this part of the configuration added automatically.

Once you have access to the CLI, you can enter instructions for specific tasks that can be found throughout the FortiOS Handbook. You can also refer to the CLI Portal for a list of the available commands.

Command syntax

When entering a command, the command line interface (CLI) requires that you use valid syntax and conform to expected input constraints. It will reject invalid commands.

Fortinet documentation uses the conventions below to describe valid command syntax.

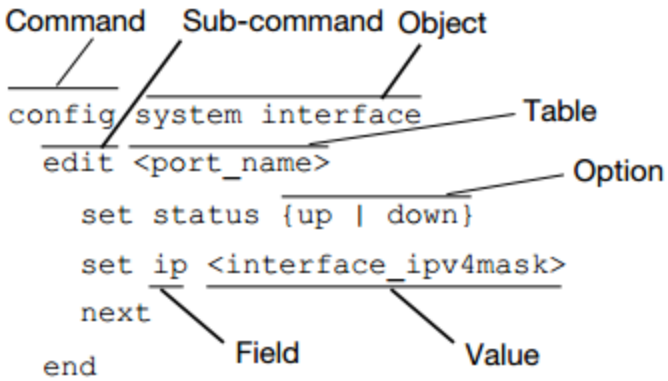
Terminology

Each command line consists of a command word that is usually followed by words for the configuration data or other specific item that the command uses or affects:

```
get system admin
```

To describe the function of each word in the command line, especially if that nature has changed between firmware versions, Fortinet uses terms with the following definitions.

Command syntax terminology



- **command** — A word that begins the command line and indicates an action that the FortiGate unit should perform on a part of the configuration or host on the network, such as `config` or `execute`. Together with other words, such as fields or values, that end when you press the Enter key, it forms a command line. Exceptions include multiline command lines, which can be entered using an escape sequence.
  Valid command lines must be unambiguous if abbreviated. Optional words or other command line permutations are indicated by syntax notation.
- **sub-command** — A kind of command that is available only when nested within the scope of another command. After entering a command, its applicable sub-commands are available to you until you exit the scope of the command, or until you descend an additional level into another sub-command. Indentation is used to indicate levels of nested commands.
  Not all top-level commands have sub-commands. Available sub-commands vary by their containing scope.
- **object** — A part of the configuration that contains tables and / or fields. Valid command lines must be specific enough to indicate an individual object.
- **table** — A set of fields that is one of possibly multiple similar sets which each have a name or number, such as an administrator account, policy, or network interface. These named or numbered sets are sometimes referenced by other parts of the configuration that use them.
- **field** — The name of a setting, such as `ip` or `hostname`. Fields in some tables must be configured with values. Failure to configure a required field will result in an invalid object configuration error message, and the FortiGate unit will discard the invalid table.
- **value** — A number, letter, IP address, or other type of input that is usually your configuration setting held by a field. Some commands, however, require multiple input values which may not be named but are simply entered in sequential order in the same command line. Valid input types are indicated by constraint notation.
- **option** — A kind of value that must be one or more words from of a fixed set of options.

Indentation

Indentation indicates levels of nested commands, which indicate what other sub-commands are available from within the scope. For example, the `edit` sub-command is available only within a command that affects tables, and the `next` sub-command is available only from within the `edit` sub-command:

```
config system interface
   edit port1
      set status up
      end
```

Notation

Brackets, braces, and pipes are used to denote valid permutations of the syntax. Constraint notations, such as `<address_ipv4>`, indicate which data types or string patterns are acceptable value input.

Command syntax notation

Convention	Description
Square brackets `[ ]`	A non-required word or series of words. For example: `[verbose {1 | 2 | 3}]` indicates that you may either omit or type both the `verbose` word and its accompanying option, such as `verbose 3`.
Angle brackets `< >`	A word constrained by data type. The angled brackets contain a descriptive name followed by an underscore (_) and suffix that indicates the valid data type. For example, `<retries_int>`, indicates that you should enter a number of retries, such as `5`. Data types include: • `<xxx_name>`: A name referring to another part of the configuration, such as `policy_A`. • `<xxx_index>`: An index number referring to another part of the configuration, such as `0` for the first static route. • `<xxx_pattern>`: A regular expression or word with wild cards that matches possible variations, such as `*@example.com` to match all email addresses ending in `@example.com`. • `<xxx_fqdn>`: A fully qualified domain name (FQDN), such as `mail.example.com`. • `<xxx_email>`: An email address, such as `admin@example.com`. • `<xxx_ipv4>`: An IPv4 address, such as `192.168.1.99`. • `<xxx_v4mask>`: A dotted decimal IPv4 netmask, such as `255.255.255.0`. • `<xxx_ipv4mask>`: A dotted decimal IPv4 address and netmask separated by a space, such as `192.168.1.99 255.255.255.0`. • `<xxx_ipv4/mask>`: A dotted decimal IPv4 address and CIDR-notation netmask separated by a slash, such as `192.168.1.1/24` • `<xxx_ipv4range>` : A hyphen (`-`)-delimited inclusive range of IPv4 addresses, such as `192.168.1.1-192.168.1.255`. • `<xxx_ipv6>`: A colon(`:`)-delimited hexadecimal IPv6 address, such as `3f2e:6a8b:78a3:0d82:1725:6a2f:0370:6234`. • `<xxx_v6mask>`: An IPv6 netmask, such as `/96`.
	• `<xxx_ipv6mask>`: A dotted decimal IPv6 address and netmask separated by a space. • `<xxx_str>`: A string of characters that is not another data type, such as `P@ssw0rd`. Strings containing spaces or special characters must be surrounded in quotes or use escape sequences. • `<xxx_int>`: An integer number that is **not** another data type, such as `15` for the number of minutes.

Convention	Description
Curly braces `{ }`	A word or series of words that is constrained to a set of options delimited by either vertical bars or spaces. You must enter at least one of the options, unless the set of options is surrounded by square brackets `[ ]`.
Options delimited by vertical bars `|`	Mutually exclusive options. For example: `{enable | disable}` indicates that you must enter either `enable` or `disable`, but must not enter both.

Options delimited by spaces	Non-mutually exclusive options. For example:
	`{http https ping snmp ssh telnet}`
	indicates that you may enter all or a subset of those options, in any order, in a space-delimited list, such as:
	`ping https ssh`

kbSub-commands

Each command line consists of a command word that is usually followed by words for the configuration data or other specific item that the command uses or affects:

```
get system admin
```

Sub-commands are available from within the scope of some commands. When you enter a sub-command level, the command prompt changes to indicate the name of the current command scope. For example, after entering:

```
config system admin
```

the command prompt becomes:

```
(admin)#
```

Applicable sub-commands are available to you until you exit the scope of the command, or until you descend an additional level into another sub-command.

For example, the `edit` sub-command is available only within a command that affects tables; the `next` sub-command is available only from within the `edit` sub-command:

```
config system interface
   edit port1
      set status up
      next
   end
```

Sub-command scope is indicated by indentation.

Available sub-commands vary by command. From a command prompt within `config`, two types of sub-commands might become available:

- commands affecting fields
- commands affecting tables

Commands for tables

clone <table>	Clone (or make a copy of) a table from the current object.
	
	For example, in `config firewall policy`, you could enter the following command to clone security policy 27 to create security policy 30:
	
	`clone 27 to 30`
	
	In `config antivirus profile`, you could enter the following command to clone an antivirus profile named `av_pro_1` to create a new antivirus profile named `av_pro_2`:
	
	`clone av_pro_1 to av_pro_2`
	
	`clone` may not be available for all tables.

delete <table>	Remove a table from the current object. For example, in `config system admin`, you could delete an administrator account named `newadmin` by typing `delete newadmin` and pressing Enter. This deletes `newadmin` and all its fields, such as `newadmin`'s `first-name` and `email-address`. `delete` is only available within objects containing tables.

edit <table>	Create or edit a table in the current object. For example, in `config system admin`: • edit the settings for the default `admin` administrator account by typing `edit admin`. • add a new administrator account with the name `newadmin` and edit `newadmin`'s settings by typing `edit newadmin`. `edit` is an interactive sub-command: further sub-commands are available from within `edit`. `edit` changes the prompt to reflect the table you are currently editing. `edit` is only available within objects containing tables. In objects such as security policies, `<table>` is a sequence number. To create a new entry without the risk of overwriting an existing one, enter `edit 0`. The CLI initially confirms the creation of entry 0, but assigns the next unused number after you finish editing and enter `end`.
end	Save the changes to the current object and exit the `config` command. This returns you to the top-level command prompt.
get	List the configuration of the current object or table. • In objects, `get` lists the table names (if present), or fields and their values. • In a table, `get` lists the fields and their values. For more information on `get` commands, see the CLI Reference.
purge	Remove all tables in the current object. For example, in `config user local`, you could type `get` to see the list of user names, then type `purge` and then `y` to confirm that you want to delete all users. `purge` is only available for objects containing tables. **Caution:** Back up the FortiGate before performing a `purge`. `purge` cannot be undone. To restore purged tables, the configuration must be restored from a backup. **Caution:** Do not purge `system interface` or `system admin` tables. `purge` does not provide default tables. This can result in being unable to connect or log in, requiring the FortiGate unit to be formatted and restored.

rename <table> to <table>	Rename a table. For example, in `config system admin`, you could rename `admin3` to `fwadmin` by typing `rename admin3 to fwadmin`. `rename` is only available within objects containing tables.
show	Display changes to the default configuration. Changes are listed in the form of configuration commands.

Example of table commands

From within the `system admin` object, you might enter:

```
edit admin_1
```

The CLI acknowledges the new table, and changes the command prompt to show that you are now within the `admin_1` table:

```
new entry 'admin_1' added
(admin_1)#
```

Commands for fields

abort	Exit both the `edit` and/or `config` commands without saving the fields.
append	Add an option to an existing list.
end	Save the changes made to the current table or object fields, and exit the `config` command. (To exit without saving, use `abort` instead.)
get	List the configuration of the current object or table. • In objects, `get` lists the table names (if present), or fields and their values. • In a table, `get` lists the fields and their values.
move	Move an object within a list, when list order is important. For example, rearranging security policies within the policy list.
next	Save the changes you have made in the current table's fields, and exit the `edit` command to the object prompt. (To save and exit completely to the root prompt, use `end` instead.) `next` is useful when you want to create or edit several tables in the same object, without leaving and re-entering the `config` command each time. `next` is only available from a table prompt; it is not available from an object prompt.

select	Clear all options except for those specified. For example, if a group contains members A, B, C, and D and you remove all users except for B, use the command `select member B`.
set <field> <value>	Set a field's value. For example, in `config system admin`, after typing `edit admin`, you could type `set password newpass` to change the password of the `admin` administrator to `newpass`. **Note:** When using `set` to change a field containing a space-delimited list, type the whole new list. For example, `set <field> <new-value>` will replace the list with the `<new-value>` rather than appending `<new-value>` to the list.
show	Display changes to the default configuration. Changes are listed in the form of configuration commands.
unselect	Remove an option from an existing list.
unset <field>	Reset the table or object's fields to default values. For example, in `config system admin`, after typing `edit admin`, typing `unset password` resets the password of the `admin` administrator account to the default (in this case, no password).

Example of field commands

From within the `admin_1` table, you might enter:

```
set password my1stExamplePassword
```

to assign the value `my1stExamplePassword` to the `password` field. You might then enter the `next` command to save the changes and edit the next administrator's table.

Permissions

Access profiles control which CLI commands an administrator account can access. Access profiles assign either read, write, or no access to each area of the FortiGate software. To view configurations, you must have read access. To make changes, you must have write access. So, depending on the account used to log in to the FortiGate unit, you may not have complete access to all CLI commands

Unlike other administrator accounts, the `admin` administrator account exists by default and cannot be deleted. The `admin` administrator account is similar to a root administrator account. This administrator account always has full permission to view and change all FortiGate configuration options, including viewing and changing **all** other administrator accounts. Its name and permissions cannot be changed. It is the only administrator account that can reset another administrator's password without being required to enter that administrator's existing password.

Set a strong password for the `admin` administrator account, and change the password regularly. By default, this administrator account has no password. Failure to maintain the password of the `admin` administrator account could compromise the security of your FortiGate unit.

For complete access to all commands, you must log in with the administrator account named `admin`.

Tips

Basic features and characteristics of the CLI environment provide support and ease of use for many CLI tasks.

Help

To display brief help during command entry, press the question mark (?) key.

- Press the question mark (?) key at the command prompt to display a list of the commands available and a description of each command.
- Type a word or part of a word, then press the question mark (?) key to display a list of valid word completions or subsequent words, and to display a description of each.

Shortcuts and key commands

Shortcuts and key commands

Action	Keys
List valid word completions or subsequent words. If multiple words could complete your entry, display all possible completions with helpful descriptions of each.	?
Complete the word with the next available match. Press the key multiple times to cycle through available matches.	Tab
Recall the previous command. Command memory is limited to the current session.	Up arrow, or Ctrl + P
Recall the next command.	Down arrow, or Ctrl + N
Move the cursor left or right within the command line.	Left or Right arrow
Move the cursor to the beginning of the command line.	Ctrl + A

Action	Keys
Move the cursor to the end of the command line.	Ctrl + E
Move the cursor backwards one word.	Ctrl + B
Move the cursor forwards one word.	Ctrl + F
Delete the current character.	Ctrl + D
Abort current interactive commands, such as when entering multiple lines. If you are not currently within an interactive command such as `config` or `edit`, this closes the CLI connection.	Ctrl + C
Continue typing a command on the next line for a multi-line command. For each line that you want to continue, terminate it with a backslash (\ ). To complete the command line, terminate it by pressing the spacebar and then the Enter key, without an immediately preceding backslash.	\ then Enter

Command abbreviation

You can abbreviate words in the command line to their smallest number of non-ambiguous characters.

For example, the command `get system status` could be abbreviated to `g sy stat`.

Adding and removing options from lists

When adding options to a list, such as a user group, using the `set` command will remove the previous configuration. For example. if you wish to add user D to a user group that already contains members A, B, and C, the command would need to be `set member A B C D`. If only `set member D` was used, then all former members would be removed from the group.

However, there are additional commands which can be used instead of `set` for changing options in a list.

Additional commands for lists

append	Add an option to an existing list. For example, `append member` would add user D to a user group while all previous group members are retained
select	Clear all options except for those specified. For example, if a group contains members A, B, C, and D and you remove all users except for B, use the command `select member B`.

unselect	Remove an option from an existing list. For example, `unselect member A` would remove member A from a group will all previous group members are retained.

Environment variables

The CLI supports the following environment variables. Variable names are case-sensitive.

Environment variables

$USERFROM	The management access type (`ssh`, `telnet`, `jsconsole` for the **CLI Console** widget in the web-based manager, and so on) and the IP address of the administrator that configured the item.
$USERNAME	The account name of the administrator that configured the item.
$SerialNum	The serial number of the FortiGate unit.

For example, the FortiGate unit's host name can be set to its serial number.

```
config system global
   set hostname $SerialNum
end
```

Special characters

The characters <, >, (,), #, ', and " are not permitted in most CLI fields. These characters are special characters, also known as reserved characters.

You may be able to enter special character as part of a string's value by using a special command, enclosing it in quotes, or preceding it with an escape sequence — in this case, a backslash (\ ) character.

In other cases, different keystrokes are required to input a special character. If you need to enter ? as part of config, you first need to input CTRL-V. If you enter the question mark (?) without first using CTRL-V, the question mark has a different meaning in CLI: it will show available command options in that section.

For example, if you enter ? without CTRL-V:

```
edit "*.xe
token line: Unmatched double quote.
```

If you enter ? with CTRL-V:

```
edit "*.xe?"
new entry '*.xe?' added
```

Entering special characters

Character	Keys
?	Ctrl + V then ?
Tab	Ctrl + V then Tab
Space (to be interpreted as part of a string value, not to end the string)	Enclose the string in quotation marks: "`Security Administrator`". Enclose the string in single quotes: '`Security Administrator`'. Precede the space with a backslash: `Security\ Administrator`.
' (to be interpreted as part of a string value, not to end the string)	\'
" (to be interpreted as part of a string value, not to end the string)	\"
\	\\

Using grep to filter get and show command output

In many cases, the `get` and `show` (and `diagnose`) commands may produce a large amount of output. If you are looking for specific information in a large get or show command output, you can use the grep command to filter the output to only display what you are looking for. The `grep` command is based on the standard UNIX grep, used for searching text output based on regular expressions.

Use the following command to display the MAC address of the FortiGate unit internal interface:

```
get hardware nic internal | grep Current_HWaddr
Current_HWaddr             00:09:0f:cb:c2:75
```

Use the following command to display all TCP sessions in the session list and include the session list line number in the output

```
get system session list | grep -n tcp
```

Use the following command to display all lines in HTTP replacement message commands that contain `URL` (upper or lower case):

```
show system replacemsg http | grep -i url
```

There are three additional options that can be applied to grep:

```
-A <num> After
```

```
-B <num> Before
-C <num> Context
```

The option `-f` is also available to support Fortinet contextual output, in order to show the complete configuration. The following example shows the difference in output when `-f` option is used versus when it is not.

Using -f:

```
show | grep -f ldap-group1
   config user group
      edit "ldap-group1"
         set member "pc40-LDAP"
      next
   end
   config firewall policy
      edit 2
         set srcintf "port31"
         set dstintf "port32"
         set srcaddr "all"
         set action accept
         set identity-based enable
         set nat enable
         config identity-based-policy
            edit 1
               set schedule "always"
               set groups "ldap-group1"
               set dstaddr "all"
               set service "ALL"
            next
         end
      next
   end
```

Without using -f:

```
show | grep ldap-group1
   edit "ldap-group1"
      set groups "ldap-group1"
```

Language support and regular expressions

Characters such as ñ, é, symbols, and ideographs are sometimes acceptable input. Support varies by the nature of the item being configured. CLI commands, objects, field names, and options must use their exact ASCII characters, but some items with arbitrary names or values may be input using your language of choice. To use other languages in those cases, you must use the correct encoding.

Input is stored using Unicode UTF-8 encoding but is not normalized from other encodings into UTF-8 before it is stored. If your input method encodes some characters differently than in UTF-8, your configured items may not display or operate as expected.

Regular expressions are especially impacted. Matching uses the UTF-8 character values. If you enter a regular expression using another encoding, or if an HTTP client sends a request in an encoding other than UTF-8, matches may not be what you expect.

For example, with Shift-JIS, backslashes (\ ) could be inadvertently interpreted as the symbol for the Japanese yen (¥) and vice versa. A regular expression intended to match HTTP requests containing money values with a yen symbol therefore may not work it if the symbol is entered using the wrong encoding.

For best results, you should:

- use UTF-8 encoding, or
- use only the characters whose numerically encoded values are the same in UTF-8, such as the US-ASCII characters that are also encoded using the same values in ISO 8859-1, Windows code page 1252, Shift-JIS and other encodings, or
- for regular expressions that must match HTTP requests, use the same encoding as your HTTP clients.

HTTP clients may send requests in encodings other than UTF-8. Encodings usually vary by the client's operating system or input language. If you cannot predict the client's encoding, you may only be able to match any parts of the request that are in English, because regardless of the encoding, the values for English characters tend to be encoded identically. For example, English words may be legible regardless of interpreting a web page as either ISO 8859-1 or as GB2312, whereas simplified Chinese characters might only be legible if the page is interpreted as GB2312.

If you configure your FortiGate unit using other encodings, you may need to switch language settings on your management computer, including for your web browser or Telnet/SSH client. For instructions on how to configure your management computer's operating system language, locale, or input method, see its documentation.

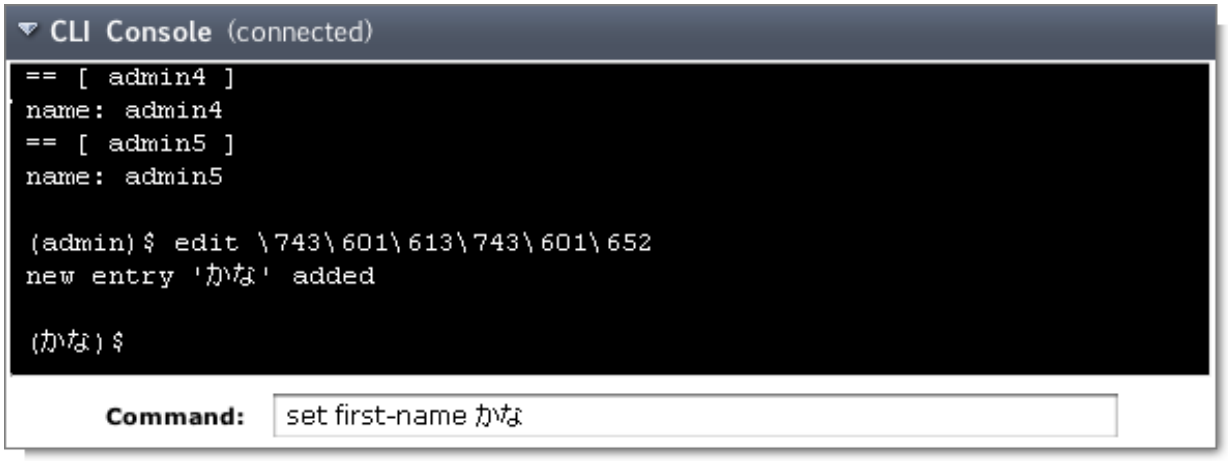
If you choose to configure parts of the FortiGate unit using non-ASCII characters, verify that all systems interacting with the FortiGate unit also support the same encodings. You should also use the same encoding throughout the configuration if possible in order to avoid needing to switch the language settings of the web-based manager and your web browser or Telnet/SSH client while you work.

Similarly to input, your web browser or CLI client should usually interpret display output as encoded using UTF-8. If it does not, your configured items may not display correctly in the GUI or CLI. Exceptions include items such as regular expressions that you may have configured using other encodings in order to match the encoding of HTTP requests that the FortiGate unit receives.

To enter non-ASCII characters in the CLI Console

1. On your management computer, start your web browser and go to the URL for the FortiGate unit's GUI.
2. Configure your web browser to interpret the page as UTF-8 encoded.
3. Log in to the FortiGate unit.
4. Open the CLI Console from the upper right-hand corner.
5. In title bar of the **CLI Console** widget, click **Edit** (the pencil icon).
6. Enable **Use external command input box**.
7. Select **OK**.
8. The **Command** field appears below the usual input and display area of the **CLI Console** .
9. In **Command**, type a command.

Entering encoded characters (CLI Console widget):



10. Press **Enter**.

    In the display area, the ***CLI Console*** widget displays your previous command interpreted into its character code equivalent, such as:

    ```
    edit \743\601\613\743\601\652
    ```

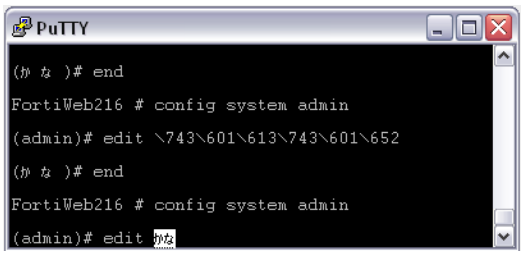
    and the command's output.

To enter non-ASCII characters in a Telnet/SSH client

1. On your management computer, start your Telnet or SSH client.
2. Configure your Telnet or SSH client to send and receive characters using UTF-8 encoding.

   Support for sending and receiving international characters varies by each Telnet/SSH client. Consult the documentation for your Telnet/SSH client.
3. Log in to the FortiGate unit.
4. At the command prompt, type your command and press Enter.

Entering encoded characters (PuTTY):



You may need to surround words that use encoded characters with single quotes (').

Depending on your Telnet/SSH client's support for your language's input methods and for sending international characters, you may need to interpret them into character codes before pressing Enter.

For example, you might need to enter:

```
edit '\743\601\613\743\601\652'
```

5. The CLI displays your previous command and its output.

Screen paging

You can configure the CLI to pause after displaying each page's worth of text when displaying multiple pages of output. When the display pauses, the last line displays `--More--`. You can then either:

- press the spacebar to display the next page.
- type `Q` to truncate the output and return to the command prompt.

This may be useful when displaying lengthy output, such as the list of possible matching commands for command completion, or a long list of settings. Rather than scrolling through or possibly exceeding the buffer of your terminal emulator, you can simply display one page at a time.

To configure the CLI display to pause when the screen is full:

```
config system console
   set output more
end
```

Baud rate

You can change the default baud rate of the local console connection.

To change the baud rate enter the following commands:

```
config system console
   set baudrate {115200 | 19200 | 38400 | 57600 | 9600}
end
```

Editing the configuration file on an external host

You can edit the FortiGate configuration on an external host by first backing up the configuration file to a TFTP server. Then edit the configuration file and restore it to the FortiGate unit.

Editing the configuration on an external host can be timesaving if you have many changes to make, especially if your plain text editor provides advanced features such as batch changes.

To edit the configuration on your computer

1. Use `execute backup` to download the configuration file to a TFTP server, such as your management computer.
2. Edit the configuration file using a plain text editor that supports Unix-style line endings.

Do not edit the first line. The first line(s) of the configuration file (preceded by a `#` character) contains information about the firmware version and FortiGate model. If you change the model number, the FortiGate unit will reject the configuration file when you attempt to restore it.

3. Use `execute restore` to upload the modified configuration file back to the FortiGate unit.

   The FortiGate unit downloads the configuration file and checks that the model information is correct. If it is, the FortiGate unit loads the configuration file and checks each command for errors. If a command is invalid, the FortiGate unit ignores the command. If the configuration file is valid, the

FortiGate unit restarts and loads the new configuration.

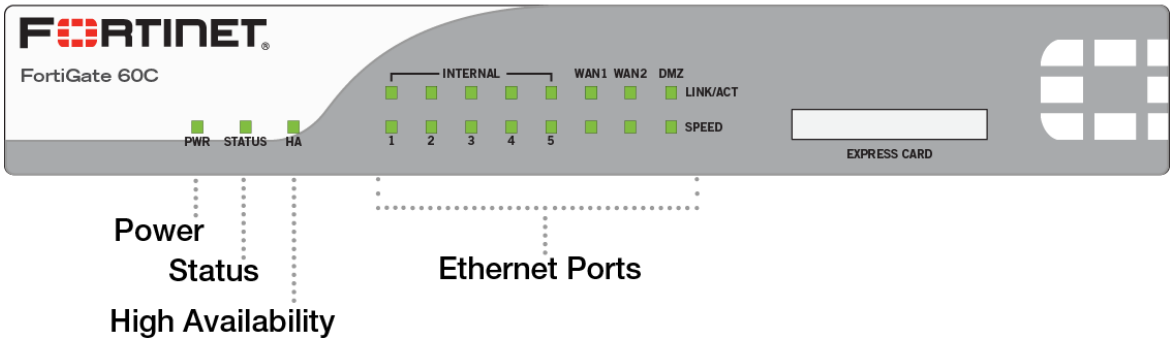
FortiGate LED Specifications

This is a guide to FortiGate LED status indicators.

Sample FortiGate Faceplates

The faceplates indicate where the LEDs are typically found on desktop and mid-range FortiGate models.

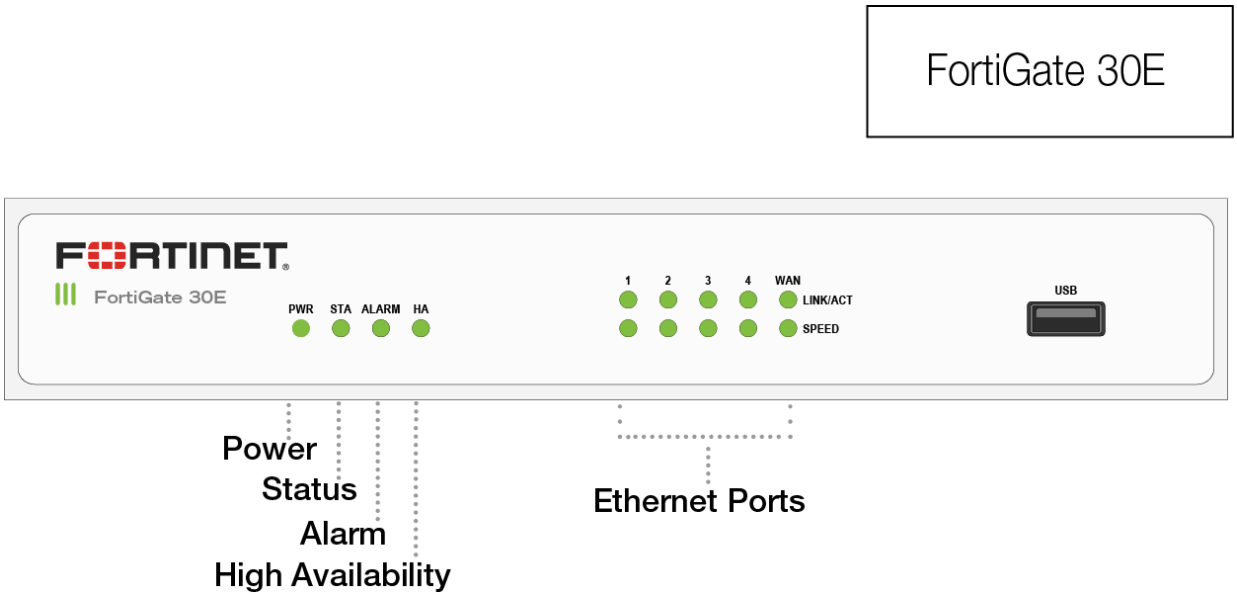
FortiGate 60C



Power
Status
High Availability
Ethernet Ports

FortiGate 100D

Alarm
Status
Power
High Availability
Ethernet Ports
SFP Ports



LED Status Codes

LABEL	STATE	MEANING
PWR	Green	Power is On.
	Off	Power is Off.
STA	Green	Normal status.
	Flashing Green	Booting Up. If the FortiGate has a reset button, Flashing Green also means that the reset button was used.
	Red	The FortiGate has a critical alarm (see About Alarm Levels).
ALARM	Off	No alarms or the FortiGate has a minor alarm.
	Amber	The FortiGate has a major alarm.
	Red	The FortiGate has a critical alarm. The status LED will also be red.
		More information at About Alarm Levels.

LABEL	STATE	MEANING
HA	Green	FortiGate is operating in an FGCP HA cluster.
	Red	A failover has occurred.
	Off	HA not configured.
		Failover operation feature not available in all units.
WIFI	Green	Wireless port is active.
	Flashing Green	Wireless interface is transmitting and receiving data.
	Off	Wireless interface is down.

About Alarm Levels

Minor, major, and critical alarms are defined based on IPMI, ATCA, and Telco standards for naming alarms.

- A minor alarm (also called an IPMI non-critical (NC) alarm) indicates a temperature or a power level outside of the normal operating range that is not considered a problem. In the case of a minor temperature alarm, the system could respond by increasing fan speed. A non-critical threshold can be an upper non-critical (UNC) threshold (for example, a high temperature or a high power level) or a lower non-critical (UNC) threshold (for example, a low power level). The LEDs do not indicate minor alarms since user intervention is not required.
- A major alarm (also called an IPMI critical or critical recoverable(CR) alarm) indicates that the system itself cannot correct the cause for the alarm and that intervention is required. For example, the cooling system cannot provide enough cooling to reduce the temperature. It could also mean that conditions (temperature, for example) are approaching the outside limit of the allowed operating range. A critical threshold can also be an upper critical (UC) threshold (for example, a high temperature or a high power level) or a lower critical (LC) threshold (for example, a low power level).
- A critical alarm (also called and IPMI non-recoverable (NR) alarm) indicates detection of a temperature or power level that is outside of the allowed operating range and could potentially cause physical damage.

LED Status Codes for Ports

TYPE OF PORT	STATE	MEANING
Ethernet Ports Link / Activity	Green	Connected.
	Flashing Green	Transmitting and receiving data.
	Off	No link established.
		On FortiGate models with front-facing ports, this LED is to the left of the port. On FortiGate models with ports at the back of the device, this LED is in the upper row.
Ethernet Ports Speed	Green	Connected at 1Gbps.
	Amber	Connected at 100Mbps.
	Off	Not connected or connected at 10Mbps.
		On FortiGate models with front-facing ports, this LED is to the right of the port. On FortiGate models with ports at the back of the device, this LED is in the lower row.
SFP Ports	Green	Connected.
	Flashing Green	Transmitting and receiving data.
	Off	No link established.

FortiGate Inspection Mode

To control your FortiGate's security profile inspection mode in FortiOS 5.6, you can select **Flow** or **Proxy Inspection Mode** from **System > Settings**. Having control over flow and proxy mode is helpful if you want to ensure that only flow inspection mode is used.

In most cases proxy mode is preferred because more security profile features are available and more configuration options for these individual features are available. Some implementations, however, may require all security profile scanning to only use flow mode. In this case, you can set your FortiGate to flow mode knowing that proxy mode inspection will not be used.

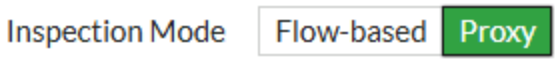
Two new policy modes are available in FortiOS 5.6.

- NGFW mode simplifies applying application control and web filtering to traffic by allowing you to add applications and web filtering thingies directly to policies.
- Transparent proxy allows you to apply web authentication to HTTP traffic without using the explicit proxy.

Setting up the FortiGate to operate in these new modes (or to operate in the other available operating modes) involves going to **System > Settings** and changing the **Inspection** and **NGFW** modes under **Operations Settings**.

Changing inspection and policy modes

To change inspection modes, go to **System > Settings** and scroll down to **Operations Settings**. You can select Flow-based to operate in Flow mode or Proxy to operate in Proxy mode.



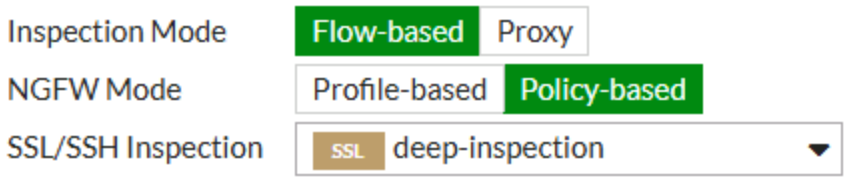
Transparent Web proxy mode

In proxy mode, FortiOS 5.6 functions just like FortiOS 5.4 with the addition of the new Transparent Web Proxy mode. See New Operating mode for Transparent web proxy (386474) on page 1.

NGFW policy mode

When you select **Flow-based** as the **Inspection Mode**, you have the option in FortiOS 5.6 to select an **NGFW Mode**. **Profile-based** mode works the same as flow-based mode did in FortiOS 5.4

In the new **NGFW Policy-based** mode, you add applications and web filtering profiles directly to a policy without having to first create and configure Application Control or Web Filtering profiles. See NGFW Policy Mode (371602) on page 1.



When you change to flow-based inspection, all proxy mode profiles are converted to flow mode, removing any proxy settings. And proxy-mode only features (for example, Web Application Profile) are removed from the GUI.

If your FortiGate has multiple VDOMs, you can set the inspection mode independently for each VDOM. Go to **System > VDOM**. Click **Edit** for the VDOM you wish to change and select the **Inspection Mode**.

CLI syntax

The following CLI commands can be used to configure inspection and policy modes:

```
config system settings
   set inspection-mode {proxy | flow}
   set policy-mode {standard | ngfw}
end
```

Security profile features mapped to inspection mode

The table below lists FortiOS security profile features and shows whether they are available in flow-based or proxy-based inspection modes.

Security Profile Feature	Flow-based inspection	Proxy-based inspection
AntiVirus	x	x
Web Filter	x	x
DNS Filter	x	x
Application Control	x	x
Intrusion Protection	x	x
Anti-Spam		x
Data Leak Protection		x
VoIP		x
ICAP		x
Web Application Firewall		x

Security Profile Feature	Flow-based inspection	Proxy-based inspection
FortiClient Profiles	x	x
Proxy Options		x
SSL/SSH Inspection	x	x
Web Rating Overrides	x	x
Web Profile Overrides		x

From the GUI, you can only configure antivirus and web filter security profiles in proxy mode. From the CLI you can configure flow-based antivirus profiles, web filter profiles and DLP profiles and they will appear on the GUI and include their inspection mode setting. Also, flow-based profiles created when in flow mode are still available when you switch to proxy mode.

In flow mode, antivirus and web filter profiles only include flow-mode features. Web filtering and virus scanning is still done with the same engines and to the same accuracy, but some inspection options are limited or not available in flow mode. Application control, intrusion protection, and FortiClient profiles are not affected when switching between flow and proxy mode.

Even though VoIP profiles are not available from the GUI in flow mode, the FortiGate can process VoIP traffic. In this case the appropriate session helper is used (for example, the SIP session helper).

Setting flow or proxy mode doesn't change the settings available from the CLI. However, when in flow mode you can't save security profiles that are set to proxy mode.

You can also add proxy-only security profiles to firewall policies from the CLI. So, for example, you can add a VoIP profile to a security policy that accepts VoIP traffic. This practice isn't recommended because the setting will not be visible from the GUI.

Proxy mode and flow mode antivirus and web filter profile options

The following tables list the antivirus and web filter profile options available in proxy and flow modes.

Antivirus features in proxy and flow mode

Feature	Proxy	Flow
Scan Mode (Quick or Full)	no	yes
Detect viruses (Block or Monitor)	yes	yes
Inspected protocols	yes	no (all relevant protocols are inspected)
Inspection Options	yes	yes (not available for quick scan mode)
Treat Windows Executables in Email Attachments as Viruses	yes	yes

Feature	Proxy	Flow
Send Files to FortiSandbox Appliance for Inspection	yes	yes
Use FortiSandbox Database	yes	yes
Include Mobile Malware Protection	yes	yes

Web Filter features in proxy and flow mode

Feature		Proxy	Flow
FortiGuard category based filter		yes	yes (show, allow, monitor, block)
Category Usage Quota		yes	no
Allow users to override blocked categories (on some models)		yes	no
Search Engines		yes	no
	Enforce 'Safe Search' on Google, Yahoo!, Bing, Yandex	yes	no
	Restrict YouTube Access	yes	no
	Log all search keywords	yes	no
Static URL Filter		yes	yes
	Block invalid URLs	yes	no
	URL Filter	yes	yes
	Block malicious URLs discovered by FortiSandbox	yes	yes
	Web Content Filter	yes	yes
Rating Options		yes	yes
	Allow websites when a rating error occurs	yes	yes
	Rate URLs by domain and IP Address	yes	yes
	Block HTTP redirects by rating	yes	no
	Rate images by URL	yes	no

Feature		Proxy	Flow
Proxy Options		yes	no
	Restrict Google account usage to specific domains	yes	no
	Provide details for blocked HTTP 4xx and 5xx errors	yes	no
	HTTP POST Action	yes	no
	Remove Java Applets	yes	no
	Remove ActiveX	yes	no
	Remove Cookies	yes	no
	Filter Per-User Black/White List	yes	no

Basic Administration

This section contains information about basic FortiGate administration that can be done after you have installed the unit in your network.

While this section mainly focuses on accomplishing tasks with the GUI, some tasks include instructions to use the command line interface (CLI). The CLI console widget is no longer part of the **Dashboard** with FortiOS 5.6. It can be accessed, however, from the upper-right hand corner of the screen and is no longer a pop-out window but a sliding window.

You can also access the CLI through FortiExplorer, or by connecting using a SSH or Telnet connection. For more information about the CLI, see Using the CLI.

The following topics are included in this section:

- Registration
- System Settings
- Administrators
- Passwords
- Firmware
- Configuration Backups
- FortiGuard
- FortiCloud

Registration

In order to have full access to Fortinet Support and FortiGuard Services, you must register your FortiGate.

Registering your FortiGate:

1. Go to the **Dashboard** and locate the **Licenses**widget.
2. Click on FortiCare Support to display a pop-up window and **Register**.
3. In the pop-up window, either use an existing Fortinet Support account or create a new one. Select your **Country** and **Reseller**.
4. Select **OK**.

Passwords

Using secure passwords are vital for preventing unauthorized access to your FortiGate. When changing the password, consider the following to ensure better security:

- Do not make passwords that are obvious, such as the company name, administrator names, or other obvious word or phrase.
- Use numbers in place of letters, for example, `passw0rd`. Alternatively, spell words with extra letters, for example, **password**.
- Administrator passwords can be up to 64 characters.
- Include a mixture of letters, numbers, and upper and lower case.
- Use multiple words together, or possibly even a sentence, for example keytothehighway.
- Use a password generator.
- Change the password regularly and always make the new password unique and not a variation of the existing password, such as changing from `password` to `password1`.
- Write the password down and store it in a safe place away from the management computer, in case you forget it or ensure that at least two people know the password in the event that one person becomes ill, is away on vacation or leaves the company. Alternatively, have two different admin logins.

The encryption for administrator passwords has been upgraded from SHA1 to SHA256.

Downgrades from FortiOS versions 5.6 to 5.4 to 5.2 to 5.0 will maintain the administrator password . If you need to downgrade to FortiOS 4.3, remove the password before the downgrade, then login after the downgrade and re-set password.

Password policy

The FortiGate includes the ability to create a password policy for administrators. With this policy, you can enforce regular changes and specific criteria for a password including:

- minimum length between 8 and 64 characters.
- if the password must contain uppercase (A, B, C) and/or lowercase (a, b, c) characters.
- if the password must contain numbers (1, 2, 3).
- if the password must contain non-alphanumeric characters (!, @, #, $, %, ^, &, *, ().
- where the password applies (admin or IPsec or both).
- the duration of the password before a new one must be specified.

To create a password policy - GUI

1. Go to **System > Settings**.
2. Configure **Password Policy** settings as required.
3. Click **Apply**.

If you add a password policy or change the requirements on an existing policy, the next time that administrator logs into the FortiGate, they are prompted to update their password to meet the new requirements before proceeding to log in.

For information about recovering a lost password and enhancements to the process, see:Resetting a lost Admin password on the Fortinet Cookbook site.

Firmware

Fortinet periodically updates the FortiGate firmware to include new features and resolve important issues. After you have registered your FortiGate unit, you can download firmware updates from the support web site, https://support.fortinet.com.

Before you install any new firmware, be sure to follow the steps below:

- Review the Release Notes for a new firmware release.
- Review the Supported Upgrade Paths document to make sure the upgrade from your current image to the desired new image is supported.
- Backup the current configuration, including local certificates.
- Test the new firmware until you are satisfied that it applies to your configuration.

Installing new firmware without reviewing release notes or testing the firmware may result in changes to settings or unexpected issues.

Only FortiGate admin users and administrators whose access profiles contain system read and write privileges can change the FortiGate firmware.

Backing up the current configuration

You should always back up the configuration before installing new firmware, in case you need to restore your FortiGate configuration.

To create a local backup:

1. Go to **Dashboard** and locate the **System Information** widget.
2. Click on the **Firmware** line and select **Update firmware in System > Firmware** from the menu that appears.
3. Choose either **Local PC** or **USB Disk** to save the configuration file. The USB option will not be available if there is no USB drive in the USB port.
4. If desired, select **Encrypt configuration file**.
5. Select **OK**.

For more information, see Configuration Backups.

Restoring configuration

Rather than reconfigure the FortiGate manually, it is possible to upload a saved configuration file.

To restore your FortiGate configuration

1. Go to **Dashboard** and locate the **System Information** widget.
2. Select **[Restore]** beside **System Configuration**.
3. Choose either **Local PC** or **USB Disk** depending the location of the file.
4. Select ***Choose File*** and browse to the correct file in the file manager window.

5. If a password was associated with the configuration file, enter it in the ***Password*** field.
6. Select **Restore**.

Troubleshooting

During the installation there are some possible errors that you may come across but the solutions are usually straightforward.

.

Error message	Reason and Solution
Configuration file error	This error occurs when attempting to upload a configuration file that is incompatible with the device. This may be due to the configuration file being for a different model or being saved from a different version of firmware. **Solution**: upload a configuration file that is for the correct model of FortiGate device and the correct version of the firmware.
Invalid password	When the configuration file is saved, it can be protected by a password. The password entered during the upload process is not matching the one associated with the configuration file. **Solution**: use the correct password if the file is password protected.

Downloading firmware

Firmware images for all FortiGate units are available on the Fortinet Customer Support website, https://support.fortinet.com.

To download firmware

1. Log into the site using your user name and password.
2. Go to **Download > Firmware Images**.
3. A list of Release Notes is shown. If you have not already done so, download and review the Release Notes for the firmware you wish to upgrade your FortiGate unit to.
4. Select **HTTPS Download**.

Firmware can also be downloaded using FTP; however, as FTP is not an encrypted file transferring protocol, HTTPS downloading is recommended.

5. Navigate to find the folder for the firmware version you wish to use.
6. Select your FortiGate model from the list. If your unit is a FortiWiFi, be sure to get the appropriate firmware, which will have a filename starting with FWF.
7. Save the firmware image to your computer.

Testing new firmware

The integrity of a firmware images downloaded from Fortinet's support portal can be verified using a file checksum. A file checksum that does not match the expected value indicates a corrupt file. The corruption could be caused by errors in transfer or by file modification. A list of expected checksum values for each build of released code is available on Fortinet's support portal.

Image integrity is also verified when the FortiGate is booting up. This integrity check is done through cyclic redundancy check (CRC). If the CRC fails, the Fortinet unit will error during the boot process, preventing suboptimal operation of the device.

Lastly, firmware images are signed and the signature is attached to the code as it is built. When upgrading an image, the running OS will generate a signature and compare it with the signature attached to the image. If the signatures do not match, the new OS will not load.

Testing before installation

FortiOS enables you to test a new firmware image by installing the firmware image from a system reboot and saving it to system memory. After completing this procedure, the FortiGate unit operates using the new firmware image with the current configuration. This new firmware image is not permanently installed. The next time the FortiGate unit restarts, it operates with the originally installed firmware image using the current configuration. If the new firmware image operates successfully, you can install it permanently using the procedure Testing new firmware on page 87 .

To use this procedure, you must connect to the CLI using the FortiGate console port and a RJ-45 to DB-9 or null modem cable. This procedure temporarily installs a new firmware image using your current configuration.

For this procedure, you must install a TFTP server that you can connect to from the FortiGate internal interface. The TFTP server should be on the same subnet as the internal interface.

To test the new firmware image

1. Connect to the CLI using a RJ-45 to DB-9 or null modem cable.
2. Make sure the TFTP server is running.
3. Copy the new firmware image file to the root directory of the TFTP server.
4. Make sure the FortiGate unit can connect to the TFTP server using the `execute ping` command.
5. Enter the following command to restart the FortiGate unit:
   ```
   execute reboot
   ```
6. As the FortiGate unit reboots, press any key to interrupt the system startup. As the FortiGate unit starts, a series of system startup messages appears.
   When the following messages appears:
   ```
   Press any key to display configuration menu....
   ```
7. Immediately press any key to interrupt the system startup.

You have only 3 seconds to press any key. If you do not press a key soon enough, the FortiGate unit reboots and you must login and repeat the execute reboot command.

If you successfully interrupt the startup process, the following messages appears:

```
[G]: Get firmware image from TFTP server.
[F]: Format boot device.
[B]: Boot with backup firmware and set as default
[C]: Configuration and information
[Q]: Quit menu and continue to boot with default firmware.
    [H]: Display this list of options.
Enter G, F, Q, or H:
```

8. Type **G** to get the new firmware image from the TFTP server.

   The following message appears:

   ```
   Enter TFTP server address [192.168.1.168]:
   ```

9. Type the address of the TFTP server and press **Enter**.

   The following message appears:

   ```
   Enter Local Address [192.168.1.188]:
   ```

10. Type an IP address of the FortiGate unit to connect to the TFTP server.

    The IP address must be on the same network as the TFTP server.

Make sure you do not enter the IP address of another device on this network.

    The following message appears:

    ```
    Enter File Name [image.out]:
    ```

11. Enter the firmware image file name and press **Enter**.

    The TFTP server uploads the firmware image file to the FortiGate unit and the following appears.

    ```
    Save as Default firmware/Backup firmware/Run image without saving: [D/B/R]
    ```

12. Type `R`.

    The FortiGate image is installed to system memory and the FortiGate unit starts running the new firmware image, but with its current configuration.

You can test the new firmware image as required. When done testing, you can reboot the FortiGate unit, and the FortiGate unit will resume using the firmware that was running before you installed the test firmware.

Upgrading the firmware

Installing firmware replaces your current antivirus and attack definitions, along with the definitions included with the firmware release you are installing. After you install new firmware, make sure that antivirus and attack definitions are up to date. You can also use the CLI command `execute update-now` to update the antivirus and attack definitions. For more information, see the System Administration handbook.

Always remember to back up your configuration before making any changes to the firmware.

Be sure to read the topics on downloading and testing firmware before upgrading.

To upgrade the firmware - GUI

1. Log into the GUI as the admin administrative user.
2. Go to **Dashboard** and locate the **System Information** widget.
3. Beside **Firmware Version**, select **Update**.
4. Type the path and filename of the firmware image file, or select **Browse** and locate the file.
5. Select **OK**.

The FortiGate unit uploads the firmware image file, upgrades to the new firmware version, restarts, and displays the FortiGate login. This process takes a few minutes.

To upgrade the firmware using the CLI

Before you begin, ensure you have a TFTP server running and accessible to the FortiGate unit.

1. Make sure the TFTP server is running.
2. Copy the new firmware image file to the root directory of the TFTP server.
3. Log into the CLI.
4. Make sure the FortiGate unit can connect to the TFTP server.

   You can use the following command to ping the computer running the TFTP server. For example, if the IP address of the TFTP server is 192.168.1.168:

   ```
   execute ping 192.168.1.168
   ```

5. Enter the following command to copy the firmware image from the TFTP server to the FortiGate unit:

   ```
   execute restore image tftp <filename> <tftp_ipv4>
   ```

   Where `<name_str>` is the name of the firmware image file and `<tftp_ip4>` is the IP address of the TFTP server. For example, if the firmware image file name is `image.out` and the IP address of the TFTP server is 192.168.1.168, enter:

   ```
   execute restore image tftp image.out 192.168.1.168
   ```

   The FortiGate unit responds with the message:

   ```
   This operation will replace the current firmware version!
       Do you want to continue? (y/n)
   ```

6. Type `y`.
7. The FortiGate unit uploads the firmware image file, upgrades to the new firmware version, and restarts. This process takes a few minutes.
8. Reconnect to the CLI.
9. Update antivirus and attack definitions, by entering:

   ```
   execute update-now
   ```

Reverting to a previous firmware version

The following procedures revert the FortiGate unit to its factory default configuration and deletes any configuration settings. If you are reverting to a previous FortiOS version, you might not be able to restore the previous configuration from the backup configuration file.

Always remember to back up your configuration before making any changes to the firmware.

To revert to a previous firmware version - GUI

1. Go to **Dashboard** and locate the **System Information**widget.
2. Beside **Firmware Version**, select **Update**.
3. Type the path and filename of the firmware image file, or select **Browse** and locate the file of the previous firmware version.
4. Select **OK**.

The FortiGate unit uploads the firmware image file, reverts to the old firmware version, resets the configuration, restarts, and displays the FortiGate login. This process takes a few minutes.

To revert to a previous firmware version - CLI

Before beginning this procedure, it is recommended that you:

- back up the FortiGate unit system configuration using the command `execute backup config`
- back up the IPS custom signatures using the command `execute backup ipsuserdefsig`
- back up web content and email filtering lists

To use the following procedure, you must have a TFTP server the FortiGate unit can connect to.

1. Make sure the TFTP server is running
2. Copy the firmware image file to the root directory of the TFTP server.
3. Log into the FortiGate CLI.
4. Make sure the FortiGate unit can connect to the TFTP server execute by using the `execute ping` command.
5. Enter the following command to copy the firmware image from the TFTP server to the FortiGate unit:

   ```
   execute restore image tftp <name_str> <tftp_ipv4>
   ```

   Where `<name_str>` is the name of the firmware image file and `<tftp_ip4>` is the IP address of the TFTP server. For example, if the firmware image file name is `imagev28.out` and the IP address of the TFTP server is 192.168.1.168, enter:

   ```
   execute restore image tftp image28.out 192.168.1.168
   ```

   The FortiGate unit responds with this message:

   ```
   This operation will replace the current firmware version!
       Do you want to continue? (y/n)
   ```

6. Type `y`.

The FortiGate unit uploads the firmware image file. After the file uploads, a message similar to the following appears:

```
Get image from tftp server OK.
Check image OK.
This operation will downgrade the current firmware version!
Do you want to continue? (y/n)
```

7. Type `y`.
8. The FortiGate unit reverts to the old firmware version, resets the configuration to factory defaults, and restarts. This process takes a few minutes.
9. Reconnect to the CLI.
10. To restore your previous configuration, if needed, use the command:

```
execute restore config <name_str> <tftp_ip4>
```

11. Update antivirus and attack definitions using the command:

```
execute update-now.
```

Installing firmware from a system reboot - CLI

In the event that the firmware upgrade does not load properly and the FortiGate unit will not boot, or continuously reboots. If this occurs, it is best to perform a fresh install of the firmware from a reboot using the CLI.

This procedure installs a firmware image and resets the FortiGate unit to default settings. You can use this procedure to upgrade to a new firmware version, revert to an older firmware version, or re-install the current firmware.

To use this procedure, you must connect to the CLI using the FortiGate console port and a RJ-45 to DB-9, or null modem cable. This procedure reverts the FortiGate unit to its factory default configuration.

For this procedure you install a TFTP server that you can connect to from the FortiGate internal interface. The TFTP server should be on the same subnet as the internal interface.

Before beginning this procedure, ensure you back up the FortiGate unit configuration.

If you are reverting to a previous FortiOS version, you might not be able to restore the previous configuration from the backup configuration file.

Installing firmware replaces your current antivirus and attack definitions, along with the definitions included with the firmware release you are installing. After you install new firmware, make sure that antivirus and attack definitions are up to date.

To install firmware from a system reboot

1. Connect to the CLI using the RJ-45 to DB-9 or null modem cable.
2. Make sure the TFTP server is running.
3. Copy the new firmware image file to the root directory of the TFTP server.
4. Make sure the internal interface is connected to the same network as the TFTP server.
5. To confirm the FortiGate unit can connect to the TFTP server, use the following command to ping the computer running the TFTP server. For example, if the IP address of the TFTP server is 192.168.1.168:

```
execute ping 192.168.1.168
```

6. Enter the following command to restart the FortiGate unit.

```
execute reboot
```

The FortiGate unit responds with the following message:

```
This operation will reboot the system!
Do you want to continue? (y/n)
```

7. Type `y`.

As the FortiGate unit starts, a series of system startup messages appears. When the following messages appears:

```
Press any key to display configuration menu.....
```

Immediately press any key to interrupt the system startup.

You have only 3 seconds to press any key. If you do not press a key soon enough, the FortiGate unit reboots and you must log in and repeat the execute reboot command.

If you successfully interrupt the startup process, the following messages appears:

```
[G]: Get firmware image from TFTP server.
[F]: Format boot device.
[B]: Boot with backup firmware and set as default
[C]: Configuration and information
[Q]: Quit menu and continue to boot with default firmware.
[H]: Display this list of options.
Enter G, F, Q, or H:
```

8. Type **G** to get to the new firmware image form the TFTP server.

The following message appears:

```
Enter TFTP server address [192.168.1.168]:
```

9. Type the address of the TFTP server and press **Enter**.

The following message appears:

```
Enter Local Address [192.168.1.188]:
```

10. Type an IP address the FortiGate unit can use to connect to the TFTP server. The IP address can be any IP address that is valid for the network the interface is connected to.

Make sure you do not enter the IP address of another device on this network.

The following message appears:

```
Enter File Name [image.out]:
```

11. Enter the firmware image filename and press **Enter**.

The TFTP server uploads the firmware image file to the FortiGate unit and a message similar to the following appears:

```
Save as Default firmware/Backup firmware/Run image without saving: [D/B/R]
```

12. Type `D`.

The FortiGate unit installs the new firmware image and restarts. The installation might take a few minutes to complete.

Restore from a USB key - CLI

To restore configuration using the CLI

1. Log into the CLI.
2. Enter the following command to restore an unencrypted configuration file:

```
exec restore image usb <filename>
```

If your configuration file was encrypted, enter the following command:

```
execute restore config usb-mode <password>
```

The FortiGate unit responds with the following message:

```
This operation will replace the current firmware version!
Do you want to continue? (y/n)
```

3. Type `y`.

Configuration revision

You can you manage multiple versions of configuration files on models that have a 512 flash memory and higher. Revision control requires either a configured central management server or the local hard drive, if the model of your FortiGate has this feature. Typically, configuration backup to local drive is not available on lower-end models.

The central management server can either be a FortiManager unit or FortiCloud.

If central management is not configured on your FortiGate unit, a message appears to tell you to do one of the following:

- enable central management
- obtain a valid license.

When revision control is enabled on your FortiGate unit, and configurations backups have been made, a list of saved revisions of those backed-up configurations appears.

Configuration revisions are viewed by clicking on Click on **admin** in the upper right-hand corner of the screen and selecting **Configuration > Revisions**.

Controlled upgrade

Using a controlled upgrade, you can upload a new version of the FortiOS firmware to a separate partition in the FortiGate memory for later upgrade. The FortiGate unit can also be configured so that when it is rebooted, it will automatically load the new firmware (CLI only). Using this option, you can stage a number of FortiGate units to do an upgrade simultaneously to all devices using FortiManager or script.

To load the firmware for later installation - GUI

1. Go to **Dashboard**.
2. Under **System Information > Firmware Version**, select **Update**.

3. Type the path and filename of the firmware image file, or select **Browse** and locate the file.
4. Deselect the **Boot the New Firmware** option.
5. Select **OK**.

To load the firmware for later installation - CLI

```
execute restore secondary-image {ftp | tftp | usb}
```

To set the FortiGate unit so that when it reboots, the new firmware is loaded, use the CLI command…

```
execute set-next-reboot {primary | secondary}
```

… where `{primary | secondary}` is the partition with the preloaded firmware.

To trigger the upgrade using the GUI

1. Go to **> Dashboard**.
2. Under **System Information > Firmware Version**, select **Details**.
3. Select the check box for the new firmware version.
   The **Comments** column indicates which firmware version is the current active version.
4. Select **Upgrade** icon.

Configuration Backups

Once you successfully configure the FortiGate, it is extremely important that you backup the configuration. In some cases, you may need to reset the FortiGate to factory defaults or perform a TFTP upload of the firmware, which will erase the existing configuration. In these instances, the configuration on the device will have to be recreated, unless a backup can be used to restore it. You should also backup the local certificates, as the unique SSL inspection CA and server certificates that are generated by your FortiGate by default are not saved in a system backup.

It is also recommended that you backup the configuration after *any* future changes are made, to ensure you have the most current configuration available. Also, backup the configuration before any upgrades of the FortiGate's firmware. Should anything happen to the configuration during the upgrade, you can easily restore the saved configuration.

Always backup the configuration and store it on the management computer or off-site. You have the option to save the configuration file to various locations including the local PC, USB key, FTP and TFTP site.The last two are configurable through the CLI only.

If you have VDOMs, you can back up the configuration of the entire FortiGate or only a specific VDOM. Note that if you are using FortiManager or FortiCloud, full backups are performed and the option to backup individual VDOMs will not appear.

Backing up the configuration using the GUI

1. Click on **admin** in the upper right-hand corner of the screen and select **Configuration > Backup**.
2. Direct the backup to your **Local PC** or to a **USB Disk**.
   The **USB Disk** option will be grayed out if no USB drive is inserted in the USB port. You can also backup to the FortiManager using the CLI.
3. If VDOMs are enabled, select to backup the entire FortiGate configuration (**Full Config**) or only a specific VDOM configuration (**VDOM Config**).
4. If backing up a VDOM configuration, select the VDOM name from the list.
5. Select **Encryption**.
   Encryption must be enabled on the backup file to back up VPN certificates.
6. Enter a password and enter it again to confirm it. You will need this password to restore the file.
7. Select **OK**.
8. The web browser will prompt you for a location to save the configuration file. The configuration file will have a .conf extension.

Backing up the configuration using the CLI

Use the following command:

```
execute backup config management-station <comment>
```

… or …

```
execute backup config usb <backup_filename> [<backup_password>]
```

… or for FTP, note that port number, username are optional depending on the FTP site…

```
execute backup config ftp <backup_filename> <ftp_server> [<port>] [<user_name>]
    [<password>]
```

… or for TFTP …

```
execute backup config tftp <backup_filename> <tftp_servers> <password>
```

Use the same commands to backup a VDOM configuration by first entering the commands:

```
config vdom
   edit <vdom_name>
```

Backup and restore the local certificates

This procedure exports a server (local) certificate and private key together as a password protected PKCS12 file. The export file is created through a customer-supplied TFTP server. Ensure that your TFTP server is running and accessible to the FortiGate before you enter the command.

Backing up the local certificates

Connect to the CLI and use the following command:

```
execute vpn certificate local export tftp <cert_name> <filename> <tftp_ip>
```

where:

- `<cert_name>` is the name of the server certificate.
- `<filename>` is a name for the output file.
- `<tftp_ip>` is the IP address assigned to the TFTP server host interface.

Restoring the local certificates - GUI

1. Move the output file from the TFTP server location to the management computer.
2. Go to **System > Certificates** and select **Import**.
3. Select the appropriate **Type** of certificate and fill in any required fields.
4. Select **Browse**. Browse to the location on the management computer where the exported file has been saved, select the file and select **Open**.
5. If required, enter the **Password** needed to upload the exported file.
6. Select **OK**.

Restoring the local certificates - CLI

Connect to the CLI and use the following command:

```
execute vpn certificate local import tftp <filename> <tftp_ip>
```

Backup and restore a configuration file using SCP

You can use secure copy protocol (SCP) to download the configuration file from the FortiGate as an alternative method of backing up the configuration file or an individual VDOM configuration file. This is done by enabling SCP for and administrator account and enabling SSH on a port used by the SCP client application to connect to the FortiGate. SCP is enabled using the CLI commands:

```
config system global
```

```
   set admin-scp enable
end
```

Use the same commands to backup a VDOM configuration by first entering the commands:

```
config global
   set admin-scp enable
end
config vdom
   edit <vdom_name>
```

Enable SSH access on the interface

SCP uses the SSH protocol to provide secure file transfer. The interface you use for administration must allow SSH access.

To enable SSH - GUI:

1. Go to **Network > Interfaces**.
2. Select the interface you use for administrative access and select **Edit**.
3. In the **Administrative Access** section, select **SSH**.
4. Select **OK**.

To enable SSH - CLI:

```
config system interface
   edit <interface_name>
      set allowaccess ping https ssh
end
```

When adding to, or removing a protocol, you must type the entire list again. For example, if you have an access list of HTTPS and SSH, and you want to add PING, typing:

```
set allowaccess ping
```

...only PING will be set. In this case, you must type...

```
set allowaccess https ssh ping
```

Using the SCP client

The FortiGate downloads the configuration file as `sys_conf`. Use the following syntax to download the file:

Linux

```
scp admin@<FortiGate_IP>:fgt-config <location>
```

Windows

```
pscp admin@<FortiGate_IP>:fgt-config <location>
```

The following examples show how to download the configuration file from a FortiGate-100D, at IP address 172.20.120.171, using Linux and Windows SCP clients.

Linux client example

To download the configuration file to a local directory called `~/config`, enter the following command:

```
scp admin@172.20.120.171:fgt-config ~/config
```

Enter the admin password when prompted.

Windows client example

To download the configuration file to a local directory called c:\config, enter the following command in a Command Prompt window:

```
pscp admin@172.20.120.171:fgt-config c:\config
```

Enter the admin password when prompted.

SCP public-private key authentication

SCP authenticates itself to the FortiGate in the same way as an administrator using SSH accesses the CLI. Instead of using a password, you can configure the SCP client and the FortiGate with a public-private key pair.

To configure public-private key authentication

1. Create a public-private key pair using a key generator compatible with your SCP client.
2. Save the private key to the location on your computer where your SSH keys are stored.
   This step depends on your SCP client. The Secure Shell key generator automatically stores the private key.
3. Copy the public key to the FortiGate using the CLI commands:

   ```
   config system admin
      edit admin
         set ssh-public-key1 "<key-type> <key-value>"
      end
   ```

   `<key-type>` must be the ssh-dss for a DSA key or ssh-rsa for an RSA key. For the `<key-value>`, copy the public key data and paste it into the CLI command.

   If you are copying the key data from Windows Notepad, copy one line at a time and ensure that you paste each line of key data at the end of the previously pasted data. As well:

   - Do not copy the end-of-line characters that appear as small rectangles in Notepad.
   - Do not copy the `---- BEGIN SSH2 PUBLIC KEY ---- or Comment: "[2048-bit dsa,...]"` lines.
   - Do not copy the `---- END SSH2 PUBLIC KEY ----` line.
4. Type the closing quotation mark and press **Enter**.

Your SCP client can now authenticate to the FortiGate based on SSH keys rather than the administrator password.

Restoring a configuration using SCP

To restore the configuration using SCP, use the commands:

```
scp <local_file> <admin_user>@<FGT_IP>:fgt_restore_config
```

To use this command/method of restoring the FortiGate configuration, you need to log in as the “admin” administrator.

Restoring a configuration

Should you need to restore a configuration file, use the following steps:

To restore the FortiGate configuration - GUI

1. Click on **admin** in the upper right-hand corner of the screen and select **Configuration > Restore**.
2. Identify the source of the configuration file to be restored : your **Local PC** or a **USB Disk**.
   The **USB Disk** option will be grayed out if no USB drive is inserted in the USB port. You can restore from the FortiManager using the CLI.
3. Enter the path and file name of the configuration file, or select **Browse** to locate the file.
4. Enter a password if required.
5. Select **Restore**.

To back up the FortiGate configuration - CLI

```
execute restore config management-station normal 0
```

… or …

```
execute restore config usb <filename> [<password>]
```

… or for FTP, note that port number, username are optional depending on the FTP site…

```
execute backup config ftp <backup_filename> <ftp_server> [<port>] [<user_
    name>] [<password>]
```

… or for TFTP …

```
execute backup config tftp <backup_filename> <tftp_server> <password>
```

The FortiGate will load the configuration file and restart. Once the restart has completed, verify that the configuration has been restored.

Configuration revision

You can you manage multiple versions of configuration files on models that have a 512 flash memory and higher. Revision control requires either a configured central management server or the local hard drive, if the model of your FortiGate has this feature. Typically, configuration backup to local drive is not available on lower-end models.

The central management server can either be a FortiManager unit or FortiCloud.

If central management is not configured on your FortiGate unit, a message appears to tell you to do one of the following:

- enable central management
- obtain a valid license.

When revision control is enabled on your FortiGate unit, and configurations backups have been made, a list of saved revisions of those backed-up configurations appears.

Configuration revisions are viewed by clicking on Click on **admin** in the upper right-hand corner of the screen and selecting **Configuration > Revisions**.

Restore factory defaults

There may be a point where need to reset the FortiGate to its original defaults; for example, to begin with a fresh configuration. There are two options when restoring factory defaults. The first resets the entire device to the original out-of-the-box configuration:

To reset the FortiGate to its factory default settings - GUI

1. Go to the **Dashboard** and locate the **System Information** widget.
2. Beside **System Configuration**, select **Restore**.
3. Select **Restore Factory Defaults** at the top of the page.

You can reset using the CLI by entering the command:

```
execute factoryreset
```

When prompted, type `y` to confirm the reset.

Alternatively, in the CLI you can reset the factory defaults but retain the interface and VDOM configuration.

Use the command:

```
execute factoryreset2
```

FortiGuard

The FortiGuard Distribution Network (FDN) of servers provides updates to antivirus, antispam and IPS definitions to your FortiGate. Worldwide coverage of FortiGuard services is provided by FortiGuard service points. FortiGuard Subscription Services provide comprehensive Unified Threat Management (UTM) security solutions to enable protection against content and network level threats.

The FortiGuard team can be found around the globe, monitoring virus, spyware and vulnerability activities. As vulnerabilities are found, signatures are created and pushed to the subscribed FortiGates. The Global Threat Research Team enables Fortinet to deliver a combination of multi-layered security intelligence and provide true zero-day protection from new and emerging threats.The FortiGuard Network has data centers around the world located in secure, high availability locations that automatically deliver updates to the Fortinet security platforms to and protect the network with the most up-to-date information.

The FortiGuard services provide a number of services to monitor world-wide activity and provide the best possible security:

- **Intrusion Prevention** System (IPS) - The FortiGuard Intrusion Prevention System (IPS) uses a customizable database of more than 4000 known threats to stop attacks that evade conventional firewall defenses. It also provides behavior-based heuristics, enabling the system to recognize threats when no signature has yet been developed. It also provides more than 1000 application identity signatures for complete application control.
- **Application Control** - Application Control allows you to identify and control applications on networks and endpoints regardless of port, protocol, and IP address used. It gives you unmatched visibility and control over application traffic, even traffic from unknown applications and sources.
- **AntiVirus** -The FortiGuard AntiVirus Service provides fully automated updates to ensure protection against the latest content level threats. It employs advanced virus, spyware, and heuristic detection engines to prevent both new and evolving threats from gaining access to your network and protects against vulnerabilities.
- **Web Filtering** - Web Filtering provides Web URL filtering to block access to harmful, inappropriate, and dangerous web sites that may contain phishing/pharming attacks, malware such as spyware, or objectionable content that can expose your organization to legal liability. Based on automatic research tools and targeted research analysis, real-time updates enable you to apply highly-granular policies that filter web access based on 78 web content categories, over 45 million rated web sites, and more than two billion web pages - all continuously updated.
- **Vulnerability Scanning** - FortiGuard Services provide comprehensive and continuous updates for vulnerabilities, remediation, patch scan, and configuration benchmarks.
- **Email Filtering** - The FortiGuard Antispam Service uses both a sender IP reputation database and a spam signature database, along with sophisticated spam filtering tools on Fortinet appliances and agents, to detect and block a wide range of spam messages. Updates to the IP reputation and spam signature databases are provided continuously via the FDN.
- **Messaging Services** - Messaging Services allow a secure email server to be automatically enabled on your FortiGate to send alert email or send email authentication tokens. With the SMS gateway, you can enter phone numbers where the FortiGate will send the SMS messages. Note that depending on your carrier, there may be a slight time delay on receiving messages.
- **DNS and DDNS** - The FortiGuard DNS and DDNS services provide an efficient method of DNS lookups once subscribed to the FortiGuard network. This is the default option. The FortiGate connects automatically to the FortiGuard DNS server. If you do not register, you need to configure an alternate DNS server.

  Configure the DDNS server settings using the CLI commands:

  ```
  config system fortiguard
  ```

```
    set ddns-server-ip
    set ddns-server-port
end
```

Support Contract and FortiGuard Subscription Services

The **Support Contract** and **FortiGuard Subscription Services** sections are displayed in abbreviated form within the **License Information** widget. A detailed version is available by going to **System > FortiGuard**.

The Support Contract area displays the availability or status of your FortiGate's support contract. The status displays can be either **Unreachable, Not Registered,** or **Valid Contract**.

The FortiGuard Subscription Services area displays detailed information about your FortiGate's support contract and FortiGuard subscription services. On this page, you can also manually update the antivirus and IPS engines.

The status icons for each section Indicates the state of the subscription service. The icon corresponds to the availability description.

- **Gray (Unreachable)** – the FortiGate is not able to connect to service.
- **Orange (Not Registered)** – the FortiGate can connect, but not subscribed.
- **Yellow (Expired)** – the FortiGate had a valid license that has expired.
- **Green (Valid license)** – the FortiGate can connect to FDN and has a registered support contract. If the Status icon is green, the expiry date also appears.

Verifying your Connection to FortiGuard

If you are not getting FortiGuard web filtering or antispam services, there are a few things to verify communication to the FortiGuard Distribution Network (FDN) is working. Before any troubleshooting, ensure that the FortiGate has been registered and you or your company, has subscribed to the FortiGuard services.

Verification - GUI

The simplest method to check that the FortiGate is communicating with the FDN, is to check the **License Information** dashboard widget. Any subscribed services should have a green check mark beside them indicating that connections are successful. Any other icon indicates a problem with the connection, or you are not subscribed to the FortiGuard services.

You can also view the FortiGuard connection status by going to **System > FortiGuard**.

Verification - CLI

You can also use the CLI to see what FortiGuard servers are available to your FortiGate. Use the following CLI command to ping the FDN for a connection:

```
ping guard.fortinet.net
```

You can also use diagnose command to find out what FortiGuard servers are available:

```
diagnose debug rating
```

From this command, you will see output similar to the following:

```
Locale : english
License : Contract
Expiration : Sun Jul 24 20:00:00 2011
```

```
Hostname : service.fortiguard.net
-=- Server List (Tue Nov 2 11:12:28 2010) -=-

IP Weight      RTT Flags  TZ   Packets   Curr Lost   Total Lost
69.20.236.180  0   10     -5   77200 0           42
69.20.236.179  0   12     -5   52514     0           34
66.117.56.42   0   32     -5   34390     0 62
80.85.69.38    50  164     0   34430     0           11763
208.91.112.194 81  223 D  -8   42530     0           8129
216.156.209.26 286 241 DI -8   55602     0          21555
```

An extensive list of servers are available. Should you see a list of three to five available servers, the FortiGuard servers are responding to DNS replies to service.FortiGuard.net, but the INIT requests are not reaching FDS services on the servers.

The rating flags indicate the server status:

D	Indicates the server was found via the DNS lookup of the hostname. If the hostname returns more than one IP address, all of them will be flagged with 'D' and will be used first for INIT requests before falling back to the other servers.
I	Indicates the server to which the last INIT request was sent
F	The server has not responded to requests and is considered to have failed.
T	The server is currently being timed.

The server list is sorted first by weight and then the server with the smallest RTT is put at the top of the list, regardless of weight. When a packet is lost, it will be resent to the next server in the list.

The weight for each server increases with failed packets and decreases with successful packets. To lower the possibility of using a faraway server, the weight is not allowed to dip below a base weight, which is calculated as the difference in hours between the FortiGate and the server multiplied by 10. The further away the server is, the higher its base weight and the lower in the list it will appear.

Port assignment

FortiGates contact the FortiGuard Distribution Network (FDN) for the latest list of FDN servers by sending UDP packets with typical source ports of 1027 or 1031, and destination ports of 53 or 8888. The FDN reply packets have a destination port of 1027 or 1031.

If your ISP blocks UDP packets in this port range, the FortiGate cannot receive the FDN reply packets. As a result, the FortiGate will not receive the complete FDN server list.

If your ISP blocks the lower range of UDP ports (around 1024), you can configure your FortiGate to use higher-numbered ports, using the CLI command…

```
config system global
   set ip-src-port-range <start port>-<end port>
end
```

…where the `<start port>` and `<end port>` are numbers ranging of 1024 to 25000.

For example, you could configure the FortiGate to not use ports lower than 2048 or ports higher than the following range:

```
config system global
   set ip-src-port-range 2048-20000
end
```

Trial and error may be required to select the best source port range. You can also contact your ISP to determine the best range to use. Push updates might be unavailable if:

- there is a NAT device installed between the unit and the FDN
- your unit connects to the Internet using a proxy server.

FortiCloud is a hosted security management and log retention service for FortiGate products. It gives you a centralized reporting, traffic analysis, configuration and log retention without the need for additional hardware and software.

Configuring Antivirus and IPS Options

Go to **System > FortiGuard**, and expand the **AV and IPS Options** section to configure the antivirus and IPS options for connecting and downloading definition files.

Use override server address	Select to configure an override server if you cannot connect to the FDN or if your organization provides updates using their own FortiGuard server.
Allow Push Update	Select to allow updates sent automatically to your FortiGate when they are available
Allow Push Update status icon	The status of the FortiGate for receiving push updates: • **Gray (Unreachable)** - the FortiGate is not able to connect to push update service • **Yellow (Not Available)** - the push update service is not available with your current support license • **Green (Available)** - the push update service is allowed.
Use override push IP and Port	Available only if both **Use override server address** and **Allow Push Update** are enabled. Enter the IP address and port of the NAT device in front of your FortiGate. FDS will connect to this device when attempting to reach the FortiGate. The NAT device must be configured to forward the FDS traffic to the FortiGate on UDP port 9443.
Schedule Updates	Select this check box to enable updates to be sent to your FortiGate at a specific time. For example, to minimize traffic lag times, you can schedule the update to occur on weekends or after work hours. Note that a schedule of once a week means any urgent updates will not be pushed until the scheduled time. However, if there is an urgent update required, select the **Update Now** button.

Update Now	Select to manually initiate an FDN update.
Submit attack characteristics… (recommended)	Select to help Fortinet maintain and improve IPS signatures. The information sent to the FortiGuard servers when an attack occurs and can be used to keep the database current as variants of attacks evolve.

Manual updates

To manually update the signature definitions file, you need to first go to the Support web site at https://support.fortinet.com. Once logged in, select FortiGuard Service Updates from the Download area of the web page. The browser will present you the most current antivirus and IPS signature definitions which you can download.

Once downloaded to your computer, log into the FortiGate to load the definition file.

To load the definition file onto the FortiGate

1. Go to **System > FortiGuard**.
2. Select the **Update** link for either **AV Definitions or IPS Definitions**.
3. Locate the downloaded file and select **OK**.

The upload may take a few minutes to complete.

Automatic updates

The FortiGate can be configured to request updates from the FortiGuard Distribution Network. You can configure this to be on a scheduled basis, or with push notifications.

Scheduling updates

Scheduling updates ensures that the virus and IPS definitions are downloaded to your FortiGate on a regular basis, ensuring that you do not forget to check for the definition files yourself. Note that updating definitions can cause a very short disruption in traffic currently being scanned while the FortiGate unit applies the new signature database. Schedule updates during off-peak hours, such as evenings or weekends, when network usage is minimal, ensures that the network activity will not suffer from the added traffic of downloading the definition files.

To enable scheduled updates - GUI

1. Go to **System > FortiGuard**.
2. Click the Expand Arrow for **AV and IPS Options**.
3. Select the **Scheduled Update** check box.
4. Select the frequency of the updates and when within that frequency.
5. Select **Apply**.

To enable scheduled updates - CLI

```
config system autoupdate schedule
   set status enable
   set frequency {every | daily | weekly}
   set time <hh:mm>
   set day <day_of_week>
```

```
end
```

Push updates

Push updates enable you to get immediate updates when new virus or intrusions have been discovered and new signatures are created. This ensures that when the latest signature is available it will be sent to the FortiGate.

When a push notification occurs, the FortiGuard server sends a notice to the FortiGate that there is a new signature definition file available. The FortiGate then initiates a download of the definition file, similar to the scheduled update.

To ensure maximum security for your network, you should have a scheduled update as well as enable the push update, in case an urgent signature is created, and your cycle of the updates only occurs weekly.

To enable push updates - GUI

1. Go to **System > FortiGuard**.
2. Click the Expand Arrow for **AV and IPS Options**.
3. Select **Allow Push Update**.
4. Select **Apply**.

To enable push updates - CLI

```
config system autoupdate push-update
   set status enable
end
```

Push IP override

If the FortiGate is behind another NAT device (or another FortiGate), to ensure it receives the push update notifications, you need to use an override IP address for the notifications. To do this, you create a virtual IP to map to the external port of the NAT device.

Generally speaking, if there are two FortiGate devices as in the diagram below, the following steps need to be completed on the FortiGate NAT device to ensure the FortiGate on the internal network receives the updates:

- Add a port forwarding virtual IP to the FortiGate NAT device that connects to the Internet by going to **Firewall Objects > Virtual IP**.
- Add a security policy to the FortiGate NAT device that connects to the Internet that includes the port forwarding virtual IP.
- Configure the FortiGate on the internal network with an override push IP and port.

On the FortiGate internal device, the virtual IP is entered as the **Use push override IP** address.

To enable push update override- GUI

1. Go to **System > FortiGuard**.
2. Under **AntiVirus & IPS Updates**, enable **Accept Push Updates**.
3. Enable **Use override push**.
4. Enter the virtual IP address configured on the NAT device.
5. Select **Apply**.

To enable push updates - CLI

```
config system autoupdate push-update
   set status enable
   set override enable
   set address <vip_address>
end
```

Sending malware statistics to FortiGuard

To support following Malware trends and making zero-day discoveries, FortiGate units send encrypted statistics to FortiGuard about IPS, Application Control, and AntiVirus events detected by the FortiGuard services running on your FortiGate. FortiGuard uses the statistics collected to achieve a balance between performance and security effectiveness by moving inactive signatures to an extended signature database.

The statistics include some non-personal information that identifies your FortiGate and its country. The information is never shared with external parties. You can choose to disable the sharing of this information by entering the following CLI command.

```
config system global
   set fds-statistics disable
end
```

Configuring Web Filtering and Email Filtering Options

Go to **System > FortiGuard**, and expand arrow to view **Web Filtering and Email Filtering Options** for setting the size of the caches and ports used.

Web Filter cache TTL	Set the Time To Live value. This is the number of seconds the FortiGate will store a blocked IP or URL locally, saving time and network access traffic, checking the FortiGuard server. Once the TTL has expired, the FortiGate will contact an FDN server to verify a web address. The TTL must be between 300 and 86400 seconds.
Antispam cache TTL	Set the Time To Live value. This is the number of seconds the FortiGate will store a blocked IP or URL locally, saving time and network access traffic, checking the FortiGuard server. Once the TTL has expired, the FortiGate will contact an FDN server to verify a web address. The TTL must be between 300 and 86400 seconds.
Port Section	Select the port assignments for contacting the FortiGuard servers. Select the **Test Availability** button to verify the connection using the selected port.
To have a URL's category rating re-evaluated, please click here	Select to re-evaluate a URL’s category rating on the FortiGuard Web Filter service.

Email filtering

The FortiGuard data centers monitor and update email databases of known spam sources. With FortiGuard Anti-Spam filtering enabled, the FortiGate verifies incoming email sender address and IPs against the database, and take the necessary action as defined within the antivirus profiles.

Spam source IP addresses can also be cached locally on the FortiGate, providing a quicker response time, while easing load on the FortiGuard servers, aiding in a quicker response time for less common email address requests.

By default, the antispam cache is enabled. The cache includes a time-to-live (TTL) value, which is the amount of time an email address will stay in the cache before expiring. You can change this value to shorten or extend the time between 5 and 1,440 minutes.

To modify the antispam cache TTL - GUI

1. Go to **System > FortiGuard**.
2. Under **Filtering**, enable **Anti-Spam Cache**.
3. Enter the TTL value in minutes.
4. Select **Apply**.

To modify the Anti-Spam filter TTL - CLI

```
config system fortiguard
   set antispam-cache-ttl <integer>
end
```

Further antispam filtering options can be configured to block, allow or quarantine, specific email addresses. These configurations are available through the **Security Profiles > Antispam** menu. For more information, see the Security Profiles handbookchapter.

Online Security Tools

The FortiGuard online center provides a number of online security tools that enable you to verify or check ratings of web sites, email addresses as well as check file for viruses:

- **URL lookup** - By entering a web site address, you can see if it has been rated and what category and classification it is filed as. If you find your web site or a site you commonly go to has been wrongly categorized, you can use this page to request that the site be re-evaluated.
  https://fortiguard.com/webfilter
- **IP and signature lookup** - The IP and signature lookup enables you to check whether an IP address is blacklisted in the FortiGuard IP reputation database or whether a URL or email address is in the signature database.
  https://fortiguard.com/webfilter
- **Online virus scanner** - If you discover a suspicious file on your machine, or suspect that a program you downloaded from the Internet might be malicious you can scan it using the FortiGuard online scanner. The questionable file can be uploaded from your computer to a dedicated server where it will be scanned using FortiClient Antivirus. Only one file of up to 1 MB can be checked at any one time. All files will be forwarded to our research labs for analysis.
  https://fortiguard.com/virusscanner

- **Malware removal tools** - FortiGuard Labs developed and maintains tools to disable and remove the specific malware and related variants. Some tools have been developed to remove specific malware, often tough to remove. A universal cleaning tool, FortiCleanup, is also available for download.
  The FortiCleanup is a tool developed to identify and cleanse systems of malicious rootkit files and their associated malware. Rootkits consist of code installed on a system with kernel level privileges, often used to hide malicious files, keylog and thwart detection / security techniques. The aim of this tool is to reduce the effectiveness of such malware by finding and eliminating rootkits. The tool offers a quick memory scan as well as a full system scan. FortiCleanup will not only remove malicious files, but also can cleanse registry entries, kernel module patches, and other tricks commonly used by rootkits - such as SSDT hooks and process enumeration hiding.
  A license to use these applications is provided free of charge, courtesy of Fortinet.
  https://fortiguard.com/malwareremoval

FortiCloud

FortiCloud is a hosted security management and log retention service for FortiGate devices. It gives you centralized reporting, traffic analysis, configuration management and log retention without the need for additional hardware and software.

FortiCloud offers a wide range of features:

- **Simplified central management** FortiCloud provides a central web-based management console to manage individual or aggregated FortiGate and FortiWiFi devices. Adding a device to the FortiCloud management subscription is straightforward. FortiCloud has detailed traffic and application visibility across the whole network.
- **Hosted log retention with large default storage allocated** Log retention is an integral part of any security and compliance program but administering a separate storage system is burdensome. FortiCloud takes care of this automatically and stores the valuable log information in the cloud. Each device is allowed up to 200Gb of log retention storage. Different types of logs can be stored including Traffic, System Events, Web, Applications and Security Events.
- **Monitoring and alerting in real time** Network availability is critical to a good end-user experience. FortiCloud enables you to monitor your FortiGate network in real time with different alerting mechanisms to pinpoint potential issues. Alerting mechanisms can be delivered via email.
- **Customized or pre-configured reporting and analysis tools** Reporting and analysis are your eyes and ears into your network's health and security. Pre-configured reports are available, as well as custom reports that can be tailored to your specific reporting and compliance requirements. For example, you may want to look closely at application usage or web site violations. The reports can be emailed as PDFs and can cover different time periods.
- **Maintain important configuration information uniformly** The correct configuration of the devices within your network is essential to maintaining an optimum performance and security posture. In addition, maintaining the correct firmware (operating system) level allows you to take advantage of the latest features.
- **Service security** - All communication (including log information) between the devices and the clouds is encrypted. Redundant data centers are always used to give the service high availability. Operational security measures have been put in place to make sure your data is secure — only you can view or retrieve it.

Registration and Activation

Before you can activate a FortiCloud account, you must first register your device.

FortiCloud accounts can be registered manually through the FortiCloud website, https://www.forticloud.com, but you can easily register and activate your account directly from your FortiGate.

Activating your FortiCloud Account

1. On your device's dashboard, in the License Information widget, select the **Activate** button in the FortiCloud section.
2. A dialogue asking you to register your FortiCloud account will appear. Enter your information, view and accept the Terms and Conditions and select **Create Account**.

3. A second dialogue window will appear, asking you to enter your information to confirm your account. This will send a confirmation email to your registered email. The dashboard widget will update to show that confirmation is required.
4. Open your email, and follow the confirmation link contained in it.

Results

A FortiCloud page will open, stating that your account has been confirmed. The Activation Pending message on the dashboard will change to state the type of account you have ('1Gb Free' or '200Gb Subscription'), and will now provide a link to the FortiCloud portal.

Enabling logging to FortiCloud

1. Go to **Log & Report > Log Settings**.
2. Enable **Send Logs to FortiCloud.**
3. Select **Test Connectivity** to ensure that your FortiGate can connect to the registered FortiCloud account.
4. Under **GUI Preferences**, set **Display Logs from FortiCloud**, to see FortiCloud logs within the FortiGate's GUI.

Logging into the FortiCloud portal

Once logging has been configured and you have registered your account, you can log into the FortiCloud portal and begin viewing your logging results. There are two methods to reach the FortiCloud portal:

- If you have direct networked access to the FortiGate, you can simply open your Dashboard and check the License Information widget. Next to the current FortiCloud connection status will be a link to reach the FortiCloud Portal.
- If you do not currently have access to the FortiGate's interface, you can visit the FortiCloud website (https://forticloud.com) and log in remotely, using your email and password. It will ask you to confirm the FortiCloud account you are connecting to and then you will be granted access. Connected devices can be remotely configured using the Scripts page in the Management Tab, useful if an administrator may be away from the unit for a long period of time.

Cloud Sandboxing

FortiCloud can be used for automated sample tracking, or sandboxing, for files from a FortiGate. This allows suspicious files to be sent to be inspected without risking network security. If the file exhibits risky behavior, or is found to contain a virus, a new virus signature is created and added to the FortiGuard antivirus signature database.

Cloud sandboxing is configured by going to **System > Security Fabric**. After enabling sandbox inspection, select **Activate FortiSandbox Cloud.**

Sandboxing results will be shown in a new tab called **AV Submissions** in the FortiCloud portal. This tab will only appear after a file has been sent for sandboxing.

For more information about FortiCloud, see the FortiCloud documentation.

Next Steps

Here's a list of some resources you can check out next to help you get the most out of your newly installed and configured FortiGate.

Best Practices

The Best Practices document is a collection of guidelines to ensure the most secure and reliable operation of FortiGates in a customer environment. It is updated periodically as new issues are identified.

This document can be found at http://docs.fortinet.com/.

The Fortinet Cookbook

The Fortinet Cookbook contains a variety of step-by-step examples of how to integrate a FortiGate into your network and apply features such as security profiles, wireless networking, and VPN.

Using the Cookbook, you can go from idea to execution in simple steps, configuring a secure network for better productivity with reduced risk.

The Fortinet Cookbook can be found at http://cookbook.fortinet.com.

The Fortinet Video Library

The Fortinet Video Library contains video tutorials showing how to configure various Fortinet products, including FortiGates. Many FortiGate videos are based on recipes from the FortiGate Cookbook.

The Fortinet Video Library can be found at http://video.fortinet.com. You can also subscribe to Fortinet's YouTube channel.

The FortiOS Handbook

The FortiOS Handbook is the complete guide to FortiOS, covering a variety of FortiGate configurations. The Handbook is available as a single complete document online. Handbook chapters are also available as standalone documents.

The FortiOS Handbook can be found at http://docs.fortinet.com/.

FORTINET

High Performance Network Security